

ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ЕЁ ПРИМЕНЕНИЕ

Новое в жизни, науке, технике

Подписная научно-популярная серия

Издается ежемесячно с 1988 г.

Файл заражен!



1991

8

Новое
в жизни,
науке,
технике

ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ЕЁ ПРИМЕНЕНИЕ

Подписная
научно-
популярная
серия

8/1991

Издается
ежемесячно
с 1988 г.

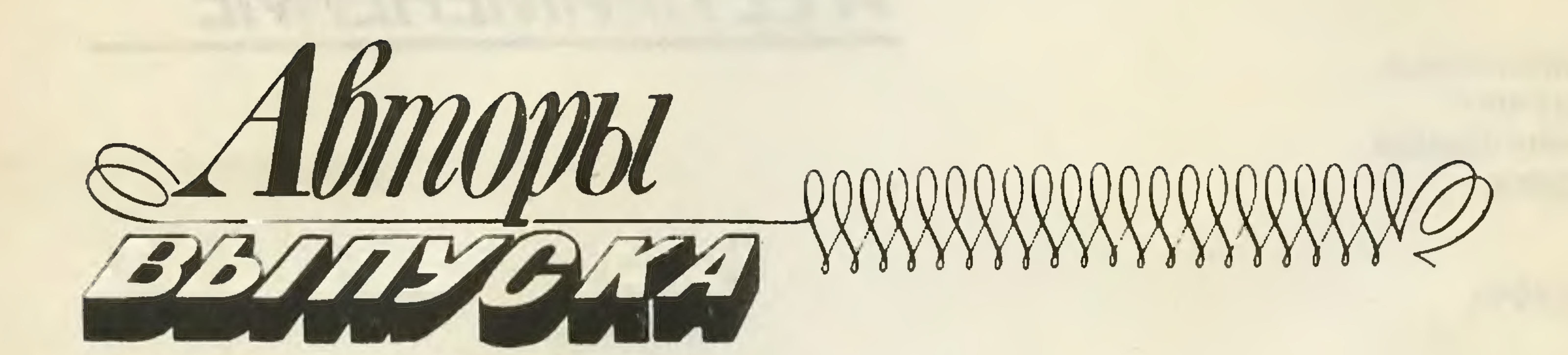
ФАЙЛ ЗАРАЖЕН!





Москва
Издательство
"Знание"
1991

ББК 32.85
Ф 38



БЕЗРУКОВ НИКОЛАЙ НИКОЛАЕВИЧ — кандидат физико-экономических наук, доцент. Один из ведущих исследователей компьютерных вирусов, руководитель семинара "Системное программирование".
САПОГОВ ВАЛЕРИЙ ВЕНИАМИНОВИЧ — научный сотрудник Чувашского Государственного университета.
УТЕНКОВ СЕРГЕЙ АЛЬБЕРТОВИЧ — инженер, жерналист.
УСЕНКОВ ДМИТРИЙ ЮРЬЕВИЧ — студент МГТУ им. Н.Э.Баумана.

Редактор Б.М.Васильев

ISBN 5-07-001720-9

© Издательство "Знание", 1991 г.



Изложена комплексная методика защиты от компьютерных вирусов, предполагающая сочетание входного контроля поступающего программного обеспечения с использованием различного рода резидентных средств защиты и систематическим архивированием. Подчеркивается значение организации архивирования, без которого любая защита иллюзорна. Обсуждаются типичные ошибки при применении средств защиты от вирусов и методика восстановления данных. Использование предлагаемой технологии позволит существенно снизить вероятность заражения, а также уничтожения ценной информации.

Н.Н.Безруков

ТЕХНОЛОГИЯ ПРИМЕНЕНИЯ СРЕДСТВ ЗАЩИТЫ ОТ ВИРУСОВ

ТЕХНОЛОГИЯ ЗАЩИТЫ ОТ ВИРУСОВ

"Предусмотрительность и осторожность одинаково важны: предусмотрительность — чтобы вовремя заметить трудности, а осторожность — чтобы самым тщательным образом подготовиться к их встрече".

Р.Амундсен

Проблема "вирус — средства защиты" аналогична проблеме "оружие нападения — оружие защиты": появление средств защиты стимулирует разработку более совершенных средств нападения. Когда появились первые вирусы, антивирусные средства как таковые, естественно, не существовали, и авторам вирусов было ни к чему применять какие-то сложные методы маскировки и обхода антивирусных средств. Однако в настоящее время вирусы должны приспособиться к среде, в которой установлены различного рода антивирусные средства, и как результат технокрысы стали применять при написании вирусов различные трюки с целью обхода наиболее популярных антивирусных средств. В целом можно ожидать, что компьютерные вирусы надолго останутся актуальной проблемой, причем совершенствование средств защиты будет сопровождаться и совершенствованием самих вирусов. Эта ситуация в какой-то мере напоминает естественный отбор, в ходе которого, как известно, выживают наиболее приспособленные. Поэтому любая система защиты должна постоянно совершенствоваться с учетом изменения "вирусной обстановки" и состоять из комплекса различных средств, взаимодополняющих и "перекрывающих" друг друга, делая тем "прорыв" какого-то одного метода или средства защиты недостаточным для проникновения вируса в систему.

Классификация средств защиты от вирусов

Время, когда можно было работать на машине и не задумываться над тем, что завтра ваших программ и файлов на диске не окажется, прошло навсегда. Впрочем, для отечественных программистов оно никогда и не наступало, поскольку надежность магнитных носителей и устройств, использовавшихся в нашей стране, всегда оставляла желать лучшего. Поэтому сейчас в арсенал каждого пользователя должен войти необходимый минимум средств защиты. Методика их применения будет рассмотрена несколько позднее. Введем необходимые термины и приведем их краткую классификацию:

архивирование: копирование таблицы FAT, ежедневное ведение архивов измененных файлов. Это самый важный, основной метод защиты от вирусов. Остальные методы не могут заменить ежедневное архивирование, хотя и повышают общий уровень защиты;

входной контроль: проверка поступающих программ детекторами, проверка соответствия длины и контрольных сумм

в сертификате длинам и контрольным суммам полученных программ; систематическое обнуление первых трех байтов сектора начальной загрузки на полученных незагружаемых дискетах (для уничтожения бутовых вирусов);

профилактика: работа с дискетами, защищенными от записи, минимизация периодов доступности дискеты для записи, разделение "общих" дискет между конкретными пользователями и разделение передаваемых и поступающих дискет, раздельное хранение вновь полученных программ и эксплуатировавшихся ранее, хранение программ на "винчестере" в архивированном виде;

ревизия: анализ вновь полученных программ специальными средствами, контроль целостности с помощью регулярного подсчета контрольных сумм и проверки сектора начальной загрузки перед считыванием информации или загрузкой с дискеты, контроль содержимого системных файлов (прежде всего COMMAND.COM) и др. Имеется целый ряд программ-ревизоров, обеспечивающих подсчет контрольных сумм (см. приложение);

карантин: каждая новая программа, полученная без контрольных сумм, должна проходить карантин, т.е. тщательно проверяться компетентными специалистами на наличие компьютерных вирусов, и в течение определенного времени за ней должно быть организовано наблюдение. Использование специального имени пользователя в ADM (Advanced Disk Manager) при работе со вновь поступившими программами, причем для этого пользователя все остальные разделы должны быть либо невидимы, либо иметь статус READ ONLY;

сегментация: использование ADM для разбиения диска на "непотопляемые отсеки" — зоны с установленным атрибутом READ ONLY. Использование для хранения ценной информации разделов, отличных от C или D и не указываемых в PATH. Раздельное хранение исполняемых программ и баз данных;

фильтрация: применение программ-сторожей для обнаружения попыток выполнить несанкционированные действия;

вакцинирование: специальная обработка файлов, дисков, каталогов, запуск резидентных программ-вакцин, имитирующих сочетание условий, которые используются данным типом вируса для определения, заражена уже программа, диск, компьютер или нет, т.е. обманывающих вирус;

автоконтроль целостности: применение резидентных программ подсчета контрольных сумм перед запуском программ, использование в программе специальных алгоритмов, позволяющих после запуска программы определить, были внесены изменения в файл, из которого загружена программа, или нет;

терапия: дезактивация конкретного вируса в зараженных программах специальной программой-антибиотиком или восстановление первоначального состояния программ путем "выкусывания" всех экземпляров вируса из каждого зараженного файла или диска с помощью программы-фага.

Как видно из приведенного выше материала, имеется несколько типов программных средств защиты от вирусов. Если попытаться наметить иерархию этих средств по их вкладу в безопасность, то представляется, что на первом месте идут программы-архиваторы.

Основная технологическая схема защиты

"Volenum ducunt fata, nolenum trahunt"
(Желающего судьба ведет, не желающего тащит).

Латинская пословица

Проблему защиты от вирусов целесообразно рассматривать в общем контексте проблемы защиты информации от несанкционированного доступа. По данной проблеме опубликован ряд монографий, среди которых следует рекомендовать учебник Л.Д.Хофмана и монографию Сяо, Керр и Медника [Сяо 82]. Основной принцип, который должен быть положен в основу разработки технологии защиты от вирусов, состоит в создании многоуровневой распределенной системы защиты, включающей как регламентацию операций на ЭВМ, так и специальные программные и аппаратные средства. При этом обязательно должно существовать несколько уровней защиты, причем их количество может варьироваться в зависимости от ценности информации, которая обрабатывается на конкретной ЭВМ.

Как уже указывалось, важное преимущество многоуровневой защиты в том, что предоставляется возможность компенсировать недостатки, присущие тому или ино-

му отдельному средству защиты. Если вирус обойдет один вид защиты, то он может "споткнуться" на другом. Автор рекомендует схему, включающую следующие этапы:

сплошной входной контроль новых программных средств;

сегментацию информации на винчестере, обеспечивающую защиту компонент MS DOS и наиболее часто используемых системных программ от заражения;

архивирование по схеме "неделя — месяц — год";

систематическое использование ревизоров для контроля целостности информации.

Организация входного контроля нового программного обеспечения

Первым и весьма важным уровнем защиты является входной контроль поступающих программ и дискет. Подобно тому как первые захваты авиалайнеров изменили отношение к проблемам досмотра пассажиров, случаи заражения вирусами должны изменить отношение к входному контролю программ и дискет, который, к сожалению, часто еще рассматривается как необязательный. Следует отдавать себе отчет, что фактически мы столкнулись с еще одной разновидностью терроризма, и борьба с ним требует перехода к сплошному входному контролю поступающих программ и дискет. При этом "фирменные" дискеты не должны составлять исключение, так как имелись случаи поставки зараженных программ на дистрибутивных дискетах. Это особенно относится к дистрибутивам, получаемым из Юго-Восточной Азии. Конечно, вероятность последнего случая существенно меньше, чем при обычном переписывании.

Большинство известных файловых и бутовых вирусов можно выявить уже на этапе входного контроля. Эта процедура отнимает всего лишь несколько минут, сохраняя десятки часов, потраченных затем на дезинфекцию винчестера, сплошной контроль всех дискет или восстановление уничтоженной информации. Для этой цели целесообразно использовать специально подобранную батарею детекторов и фагов. Можно рекомендовать следующий состав такой батареи (приведенные ниже фаги следует использовать в режиме детектирования): Scan, LD, SOS, Aidstest, -V.

Указанную батарею можно запускать как с помощью обычного BAT-файла, так и с помощью оболочки типа антивирус-интегратора (например, AVTP). В случае обнаружения вирусов полезно отпечатать и сохранить протокол проведенного контроля. При интерпретации результатов следует учитывать возможность ложного срабатывания одного из детекторов.

Поскольку при входном контроле вирус находится в пассивном состоянии, а число анализируемых объектов невелико по сравнению с типичным содержимым винчестера, этот тип контроля представляется наиболее важным, позволяя полностью исключить случаи заражения по меньшей мере уже известными вирусами (т.е. 99% случаев).

Перед проведением входного контроля рекомендуется провести вакцинацию дискет бутовой вакциной VitaminB. Это предохранит ваш компьютер от заражения бутовым вирусом.

Понятия достоверной дистрибутивной копии и сертификата

Развитие методов маскировки вирусов делает необходимым понятие достоверной дистрибутивной копии. Здесь возникает определенная проблема, в случае если распространяемое программное обеспечение относится к классу Freeware. Главным критерием достоверности дистрибутивной копии является соответствие длины, даты и контрольной суммы файла значениям, приведенным в протоколе архивирования разработчика, если, конечно, таковой имеется или в протоколе, полученном с "только что распечатанной" дистрибутивной версии. Следует подчеркнуть важность эталонного протокола как своего рода сертификата подлинности передаваемого программного обеспечения. В настоящее время ряд архиваторов обеспечивает контроль целостности компонент архива при распаковке и выдает соответствующее сообщение в протокол разархивирования.

Если программное обеспечение получено с сертификатом, то сразу после его получения рекомендуется снять справку с архива и сравнить с сертификатом.

Контроль текстовых строк, содержащихся в файле

Рекомендуется визуально просматривать ASCII-строки, имеющиеся в полученных программах, используя Labtest, Red, Edmsg или другую подходящую утилиту. Полезно убедиться, что полученное вами программное обеспечение не содержит "подозрительных" текстовых строк типа "COMMAND.COM", "PATH=", "*.COM", "???????COM", "Kill", "Stoned", "Virus", "Stupid' и т.д. Поскольку большинство разработчиков вирусов, по-видимому, страдают "комплексом неполноценности", разработка вируса для них является патологическим способом самоутверждения. Поэтому им трудно удержаться от включения в текст сообщений подобного рода. В то же время многие вирусы шифруют содержащиеся в них строки, и они становятся видны только при трассировке программы. Однако отрицательный результат — тоже результат, и если при визуальном просмотре в последних 2-3К дампа нет ни одной текстовой строки, то это тоже должно настораживать. Если это является результатом упаковки EXE-файлов специальным упаковщиком, распаковывающим файл в оперативной памяти перед выполнением (Lzexe, Exepack и др.), то необходимо предварительно распаковать файл для анализа с помощью утилиты Unlzexe.

Использование отладчиков и дизассемблеров

Подозрительные файлы целесообразно просмотреть с помощью отладчика, позволяющего отслеживать выдаваемые программой прерывания (Periscope, Quad Analizer, AFD, Turbo Debugger и др.). В случае выявления "подозрительных" последовательностей прерываний соответствующие участки программы следует дизассемблировать и пройти в пошаговом режиме.

Следует отметить, что возникновение различного рода сложностей при прохождении программы отладчиком, например "уход из-под отладчика", зависание машины и др., обычно свидетельствуют о том, что данную программу использовать не следует. Возможно, это "взломанная" программа с остатками средств защиты от копирования. Или это троянизированная программа. При имеющемся разнообразии программных средств IBM PC наличие защиты от копирования является фактором, снижающим ценность программного продукта, и при прочих равных условиях рекомендуется использовать "незащищенные" программные продукты.

Карантинный режим

"Все, что хорошо начинается, кончается плохо. Все что начинается плохо, кончается еще хуже".

Из законов Мерфи

В случае, когда программное обеспечение получено без сертификата, из сомнительного источника или не эксплуатировалось в том месте, откуда оно было передано, первые несколько дней эксплуатации полученного программного обеспечения полезно выполнять в карантинном режиме. В этом режиме целесообразно использовать искусственно ускоренный календарь, т.е. задавать при каждом следующем эксперименте новый месяц и день недели. Это повышает вероятность обнаружения троянской компоненты, срабатывающей в определенный месяц или после истечения определенного календарного отрезка времени.

Вообще говоря, лучше всего иметь специально выделенный "карантинный" компьютер для подобного рода экспериментов. Сейчас, с уходом в тень компьютеров типа PC XT, такая возможность начинает становиться реальностью и в наших условиях. По крайней мере для наиболее богатых организаций. В этом компьютере все программное обеспечение полезно обработать, дописав в конец каждого файла специальную строку, например вида "***OK***" или ***NB <контрольная сумма без маркера> ***. Дописывание таких концевых маркеров можно выполнить автоматически, составив пакетный файл. Их наличие облегчает последующий анализ программ, поскольку граница между вирусом, "севшим" в конец программы, и файлом становится четко определенной. Конечно, это не исключает необходимости использования "джентльменского" набора антивирусных средств, включающего подходящий ревизор, сторож и самоконтролирующиеся программы-приманки. Резидентные сторожа следует использовать лишь периодически, поскольку вирус может распознавать присутствие таких средств и соответствующим образом менять свое поведение (на "карантинном" компьютере стоит задача

обнаружить момент заражения, а не препятствовать размножению вируса).

Если выделить карантинный компьютер не представляется возможным, то целесообразно создать "карантинный режим" на одном из компьютеров, не содержащем особо ценных файлов или баз данных. Вход в карантинный режим должен выполняться с помощью специального имени пользователя, которому для записи доступен лишь логический диск, и специальный карантинный раздел винчестера, а большинство остальных скрыто либо имеют статус READ ONLY. При этом для всех компонент операционной системы и некоторых утилит, используемых как приманка для вируса, следует записать в соответствующий файл контрольные суммы, вычисленные подходящим ревизором (при его отсутствии для этой цели можно использовать любой архиватор, например, Pkzip).

Для компьютеров типа PC XT, имеющих меньше 1M оперативной памяти, рекомендуется организовать из части памяти достаточно большой электронный диск (скажем, 250 K), записать на него несколько часто используемых системных утилит и "погонять" эти утилиты. Возможно, вирус "клюнет" и заразит одну из этих программ — в этом случае ревизор обнаружит несовпадение контрольных сумм и сообщит о факте заражения. Преимущество использования электронного диска для таких экспериментов связано с тем, что его содержимое автоматически уничтожается при перезагрузке или выключении питания. Это обеспечивает дополнительную гарантию, что из-за невнимательности или случайного стечения обстоятельств какая-нибудь зараженная в процессе экспериментов программа не останется на диске и затем не станет использоваться кем-нибудь другим.

Троянские компоненты в незаконно распространяемых копиях программ и программах со "сломанной" защитой

"Ах бедность, бедность, как унижает она сердце нам".

А.С.Пушкин

Известны случаи, когда в состав незаконной копии включались троянские программы. Например, одна из программ на распространявшейся в Донецке дискете с незаконной копией игры Accolade выполняла периодическое стирание CMOS-памяти. Следует отметить, что наряду с незаконно распространяемыми игровыми программами, которые часто бывают заражены вирусами, определенную опасность представляют программы со "сломанной" защитой, поскольку возможны случаи, когда снятие защиты ведет к активации троянской компоненты, заложенной в программе. При этом вы можете не подозревать, что эксплуатируемая программа является коммерческой, поскольку соответствующие сообщения при снятии защиты часто меняются или исключаются, а сама программа может быть переименована. Автору известны случаи, когда разработчики отечественных коммерческих систем защиты программ от копирования предлагали потенциальным пользователям предусмотреть действия, вызывающие разрушение информации при запуске защищенной программы "не на том" компьютере. Остается надеяться, что на это предложение никто из разработчиков не клюнул.

Известно несколько случаев распространения вируса с помощью троянской версии антивирусной программы.

После покупки компьютера проверяйте содержимое винчестера

"Опыт растет прямо пропорционально выведенному из строя оборудованию".

Из законов Мерфи

Все программное обеспечение, содержащееся на винчестере только что купленного компьютера, целесообразно рассматривать как новое. Поэтому при получении новой машины, если вы не собираетесь переформатировать винчестер, прежде всего протестируйте винчестер и все полученные дискеты на наличие вирусов. Кооперативы, перепродающие ПЭВМ, оказались одним из каналов распространения вирусов. Это связано с тем, что перед продажей компьютер часто используется как игровой автомат. Многие пользователи сообщали, что практически все программы на винчестере были заражены одним, а иногда и несколькими различными типами вирусов. При тестировании такого винчестера не забудьте загрузиться с заведомо чистой дискеты с операционной системой. Если у вас еще нет опыта работы с персональными компьютерами, желательно пригласить специалистов со сторо-

ны. Получая болгарское программное обеспечение, будьте внимательны и осторожны: возможно, некоторые программы заражены новыми типами вирусов.

Сегментация информации на винчестере

Второй уровень защиты может быть основан на сегментации винчестера с помощью специального драйвера, обеспечивающего присвоение отдельным логическим дискам (разделам винчестера) атрибута READ ONLY, а также простейшую схему парольного доступа. В качестве такого драйвера можно применять различные программы. Автор рекомендует использовать Advanced Disk Manager, который не только позволяет разбить диск на разделы, но и организовать несколько вариантов доступа к ним с помощью паролей, например при одном пароле все диски, кроме одного, не видны, при другом имеют статус READ ONLY и т.д. Кроме того, уровень обеспечиваемой им защиты от записи выше, чем других распространенных драйверов. Вместе с тем ADM не является средством защиты от несанкционированного доступа: имеется ряд программ, позволяющих переключиться в статус суперпользователя или даже выдать на экран список всех паролей.

Основные принципы сегментации информации

Как и для морских кораблей, схема размещения "непотопляемых отсеков" (разделов с установленным атрибутом READ ONLY) во многом определяет "живучесть" винчестера при внезапной атаке. Винчестер, содержащий единственный незащищенный раздел С, обычно "идет ко дну" при первой же атаке вируса или троянской программы.

Количество "непотопляемых отсеков" и их содержимое зависят от решаемых задач и объема винчестера. Для наиболее распространенных 40 М винчестеров можно использовать три-четыре раздела. При этом на логическом диске С, с которого выполняется загрузка, следует оставить лишь минимальное количество файлов (AUTOEXEC.BAT, COMMAND.COM, CONFIG.SYS, скрытые системные файлы и программы-ловушки, контролирующие свою контрольную сумму). Остальную часть винчестера следует разбить на зону трансляторов и системных утилит (раздел D также со статусом READ ONLY) и несколько разделов для отдельных пользователей (групп пользователей) с соответствующими ограничениями доступа. При этом для минимизации движения головок разделы пользователей можно расположить между разделом С (MS DOS) и разделом с трансляторами и утилитами. Размер разделов следует выбирать с учетом удобства последующей архивации (см.ниже).

Следует отметить, что, как и любая сегментация, сегментация винчестера снижает эффективность использования дискового пространства, поэтому увлекаться созданием мелких разделов не стоит.

Защита операционной системы от заражения

> *"Если какая-нибудь неприятность может случиться, она случается".*
>
> Из законов Мерфи

Важным профилактическим средством в борьбе с файловыми вирусами является "затруднение им жизни" путем исключения значительной части загрузочных модулей из сферы их досягаемости. Этот метод, называемый сегментацией, был уже кратко рассмотрен. Однако применительно к самой операционной системе сегментация настолько важна, что на ней стоит остановиться отдельно. При правильном размещении операционной системы и ряда утилит можно гарантировать, что после начальной загрузки операционной системы она еще не заражена резидентным файловым вирусом. Это создает настолько значительные удобства и преимущества, что для достижения этой цели стоит потратить время и силы на перекомпоновку винчестера, если это еще вами не сделано. Первую задачу, которую нужно выполнить при "вирусобезопасной" постановке операционной системы, — это разместить ее в защищенном от записи разделе (например, разделе D).

Следует отметить, что логический диск с операционной системой не должен быть слишком большим. Туда следует включать только саму операционную систему и некоторые "стабильные" утилиты (Norton Utilities, PC Shell и т.д.). Вопрос о включении модулей трансляторов зависит от того, насколько часто вы переходите от версии к версии и от источников получения новых версий: общий принцип состоит в компоновке

этого диска так, чтобы необходимость входить в систему с паролем, обеспечивающим возможность записи на этот диск, возникала как можно реже. Кроме того, новые полученные утилиты нельзя включать в состав этого диска без предварительной тщательной проверки и прохождения "карантинного" режима хотя бы в течение месяца. Не стоит впадать из одной крайности в другую и стремиться "защитить все подряд" — это существенно затрудняет работу и в большинстве случаев сводит на нет защиту из-за частой работы в "открытом" режиме. Оптимальное количество исполняемых файлов, защищенных от записи, вряд ли должно превышать 20 — 30% от общего количества используемых программ. В качестве критериев можно использовать целесообразность подключения соответствующего каталога к PATH, а также степень стабильности данного программного продукта.

Помимо командного процессора, одними из первых обычно заражаются файлы, входящие в AUTOEXEC.BAT. Поэтому их тоже следует размещать в разделе винчестера, имеющего статус READ ONLY. Иногда вирусы заражают файлы IBMBIO и IBMCOM. Хотя обычно при этом операционная система теряет работоспособность, здесь есть нюанс, состоящий в том, что не рекомендуется (а с помощью DM и нельзя) присваивать диску C статус READ ONLY. Поэтому файлы остаются незащищенными, и необходимо использовать ревизор для контроля их целостности, включив его запуск в AUTOEXEC.BAT. При использовании сторожа FluShot Plus следует обязательно вставить контрольные суммы для указанных файлов в соответствующий файл.

Стратегия защиты командного процессора

Поскольку командный процессор служит излюбленной мишенью для атаки файловых вирусов, нужно одновременно оставить его в качестве "мишени" и в то же время не допустить использования зараженного командного процессора при перезагрузке системы. Очевидно, что эти требования выглядят как взаимоисключающие. Однако им можно удовлетворить, если "оригинал" командного процессора разместить на защищенном от записи диске, а после начальной загрузки скопировать его на виртуальный диск и установить соответствующее значение переменной COMSPEC. Для того чтобы командный процессор в процессе начальной загрузки считывался из защищенного раздела в CONFIG.SYS, следует включить такую строку:

```
SHELL = D:\DOS\COMMAND.COM
или
SHELL = D:\4DOS\4DOS.COM @C:\4DOS.DAT
```

Последняя строка предполагает использование "альтернативного" командного процессора 4DOS (читается — FOREDOS), разработанного американской фирмой J.P. Software и распространяемого как Shareware. Этот командный процессор довольно удобен для пользователей, работающих на PC AT или PS/2, имеющих один или более мегабайт оперативной памяти. Его использование вместо стандартного COMMAND.COM обеспечивает дополнительную степень индивидуализации операционной системы (как известно, имеется по меньшей мере один вирус — Lehigh, ориентированный на заражение именно стандартного COMMAND.COM).Он обеспечивает ряд дополнительных удобств, среди которых отметим диалоговую помощь по всем командам MS DOS и существенно расширенный командный язык, значительно облегчающий программирование BAT-файлов. Кстати, диалоговый HELP от 4DOS можно использовать и со стандартным командным процессором. Как и COMMAND.COM, командный процессор 4DOS.COM сегментирован и состоит из небольшой резидентной части 4DOS.COM размером около 11K (в памяти остается всего 2.5K — меньше, чем у резидентной части COMMAND.COM) и оверлея 4DOS286.EXE размером около 64K. Шансы, что вирусу удастся заразить этот командный процессор тем же методом, что и стандартный COMMAND.COM, сравнительно невелики.

Вместе с тем не только вирусы, но и программы, привязанные к стандартному COMMAND.COM, могут оказаться неработоспособными при использовании 4DOS. Поэтому целесообразность использования указанного командного процессора во многом зависит от решаемых задач.

Запись командного процессора на виртуальный диск и переназначение переменной COMSPEC для стандартного COMMAND.COM это выполняется путем включения в качестве первых строк

AUTOEXEC.BAT двух следующих строк:

```
SET COMSPEC=E:\COMMAND.COM COPY
D:\DOS\COMMAND.COM E:
```

В приведенных строках предполагается, что логический диск Е является виртуальным. Использование виртуального диска для хранения командного процессора (в сочетании с заданием соответствующего значения параметра COMSPEC) не только превращает его в своего рода дрозофилу, заражение которой легко контролировать, а удаление которой с диска обеспечивается автоматически при перезагрузке MS DOS, но и ускоряет работу с некоторыми оболочками (например, Norton Commander). При этом целесообразно иметь специальную команду для периодического контролирования сравнения COMMAND.COM с эталоном (автор использует для этой цели специальную клавишу в пользовательском меню Norton Commander, вызываемом нажатием функциональной клавиши F2). В этом случае гораздо легче заметить изменение командного процессора.

Использование каталога BAT-файлов

Связывание длинной цепочки каталогов по PATH создает очевидные удобства при работе. В то же время такое решение имеет и два существенных недостатка. Во-первых, замедляется поиск запускаемой программы (если отсутствует кэш), а во-вторых, наличие соответствующей строки PATH облегчает файловым вирусам поиск исполняемых файлов. Поэтому рекомендуется компромиссное решение: указывать в PATH только каталоги, расположенные на защищенных от записи логических дисках, а также корневой каталог и один дополнительный каталог с BAT-файлами. В последний удобно занести файлы, указывающие путь для исполняемой программы, расположенной на незащищенных от записи логических дисках. При этом для каждой часто используемой программы удобно составить отдельный BAT-файл, в котором обычно удается предусмотреть некоторые дополнительные удобства в виде установки каких-то типовых режимов, сокращенного набора групп параметров и другой сервис, уровень которого зависит от вашей собственной изобретательности. Это существенно упрощает и ускоряет процесс работы, поскольку типовые параметры набирать не приходится, время на просмотр длинной цепочки каталогов при поиске программы не теряется. В то же время такое решение повышает безопасность, не давая вирусам легко и просто извлекать путь к жертвам из PATH.

Автор много лет проработал на ЕС ЭВМ, где использование библиотеки процедур (SYS1.PROCLIB) было стандартной практикой, и был удивлен, перейдя на персональные ЭВМ, обнаружив,что этот прием не относится к стандартным.

Архивирование

"Инженер присел и отвернул кран, чтобы смыть мыло. Кран захлебнулся и стал медленно говорить что-то неразборчивое. Вода не шла..."

И.Ильф, Е.Петров

Пользователь компьютера, не имеющий "свежего" и надежного архива содержимого своего винчестера, находится во власти случая. Этот случай может подвернуться в виде срабатывания вируса, троянской программы, в виде внезапного отключения электроэнергии, или, наконец, в виде воды, которую забыли на ночь закрыть на верхнем этаже. Пользователь, хранящий в компьютере ценную информацию, должен быть всегда настороже и, как известный герой Ю.Семенова, иметь "отходной вариант" заранее. Единственным надежным методом защиты ценной информации от превратностей судьбы является архивирование. При наличии ежедневных копий максимум, что может сделать вирус, это уничтожить результаты последнего дня вашей работы.

Состояние человека, который в одну секунду потерял содержимое винчестера, трудно описать словами. Только что машина работала, все файлы были на месте. А сейчас информация, на создание которой было потрачено столько труда, исчезла и резервной копии вообще нет. Это настоящее крушение, и по сравнению с ним ситуация, приведенная в эпиграфе, — просто пустяк. И винить, кроме самого себя, в ней некого. А ведь достаточно было потратить полчаса, чтобы все было иначе. Но поздно.

Поэтому создание архива — это далеко не та вещь, которую можно отложить на потом. В сущности, это такая же часть работы пользователя, как программирование или ведение базы данных. Однако если по вопросам программирования или базам данных написаны горы литературы, то по вопросам архивирования литературы практически нет и каждый пользователь создает собственную систему. Часто этой системой является отсутствие таковой. Ниже приводятся некоторые рекомендации, основанные на личном (и приобретенном достаточно дорогой ценой) опыте автора.

Используйте программы резервирования FAT и главного каталога в AUTOEXEC.BAT

> *"Посмотрите! Вот он без страховки идет".*
>
> В.Высоцкий

Поскольку FAT и главный каталог являются наиболее уязвимыми управляющими блоками MS DOS, необходимо предпринимать меры по их дополнительному резервированию. Такую возможность обеспечивает, в частности, программа Image из версии 5 утилит П.Нортона, вызов которой следует вставить в AUTOEXEC.BAT. Наряду с Image можно использовать более старую программу Mirror, входящую в пакет PC Shell. Она записывает копии указанных секторов в конец винчестера.

Резервирование MBR, бутсектора, FAT и каталогов важно не только в плане защиты от вирусов, но и как метод страховки на случай непредвиденного стечения обстоятельств или чьих-то (в том числе и собственных) действий. Периодически рекомендуется выгружать файлы, создаваемые этими утилитами на специальную дискету из "горячей коробки" (см. ниже). Это особенно важно, если при сжатии диска утилитой Norton Speed Disk задан режим перенесения всех каталогов в начало логического диска.

Используйте систему "неделя — месяц — год"

Желательно иметь несколько комплектов дискет для архива винчестера и вести циклическую запись на эти комплекты (например, для трех комплектов можно использовать "классический" принцип "неделя — месяц — год"). В этом случае различают главный архив, в котором хранится полный объем используемой информации и программного обеспечения, и текущие архивы, в которые заносятся только последние программные продукты и файлы. Текущих архивов может быть несколько, в зависимости от периодичности их обновления. Главный архив целесообразно обновлять примерно один раз в месяц, а текущие архивы — по крайней мере один раз в неделю.

Для создания главного архива рекомендуется использовать программу FastBack Plus (версию 2.1 или более позднюю). Она позволяет выгрузить 20М винчестер на 35 дискет по 360 К или 12 дискет по 1.2 М примерно за 20 мин. Следует отметить, что если на машине установлен дисковод 1.2 М, то использование дискет 360 К для создания архива не оправдано. Рекомендуется использовать как минимум формат 730 К, а лучше формат 800 К (80 треков, 10 секторов на трек). Обычные дискеты DS/DD работают при такой разметке достаточно надежно. Однако по возможности используйте дискеты 1.2 М, поскольку в этом случае создание архива выполняется значительно проще и быстрее, чем на дискетах 730 К. С учетом отсутствия на большинстве отечественных машин стриммеров рекомендуемый размер раздела винчестера должен соответствовать определенному количеству коробок дискет архива. Например, раздел 20 М очень удобен при создании архива на дискетах 1.2 М, поскольку 12 — 14 дискет помещаются в одну коробку, и неудобен при создании архива на дискетах 730 К (требуется примерно 18 дискет). После создания главного архива рекомендуется провести оптимизацию винчестера, например, с помощью Norton Speed Disk из 5-й версии утилит Нортона.

Для создания недельного архива рекомендуется использовать архиваторы Pkzip (версию 1.2 или более позднюю) или Lha (версию 2.05 или более позднюю). При этом каждый архив в главном каталоге диска рекомендуется сворачивать в отдельный файл. Если размер файла на дискете превышает размер дискеты, то можно воспользоваться архиватором Arj, обеспечивающим возможность выгружать архив на несколько последовательных дискет или создать архив на винчестере, а затем "разрезать" его на отдельные фрагменты утилитой Split (см.электронный бюллетень Софтпанорама 3-3, далее по тексту СП 3-3. О бюллетене Софтпанорама

см. Приложение) и записать на дискеты. При нехватке дискет в недельный архив следует включать только каталоги, измененные за прошедшую неделю.

И наконец, ежедневный архив включает все тексты, измененные за рабочий день. Выключать компьютер, не сбросив измененные тексты на дискету, не рекомендуется. Следует помнить, что винчестеры портятся не только от вирусов. Вероятность того, что, уйдя с работы сегодня, завтра вы обнаружите, что информация на винчестере не читается, не равна нулю даже для самых лучших компьютеров, а тем более для наиболее дешевых моделей, попадающих в нашу страну.

Если какой-то каталог на винчестере используется лишь эпизодически или только определенным пользователем, то после каждого использования желательно все программы в нем сворачивать архиватором типа PKARC, поскольку заразить программу, находящуюся в архиве, практически невозможно.

Очень часто процесс архивирования сводят к выгрузке с винчестера всех файлов. На самом деле архивированию подлежат и системные блоки, в частности MBR и бутсектор. Последние следует скопировать на дискету с помощью программы DiskTool 5 версии утилит П.Нортона. Кроме того, следует копировать на дискету FAT и главный каталог с помощью утилиты Mirror из PC Shell или Image из 5-й версии утилит П.Нортона. Эту операцию следует выполнять не реже одного раза в неделю, а если предполагается использование каких-то новых программ, то при загрузке ЭВМ. Как и архиваторы, программы резервирования FAT и каталогов важны не только в плане защиты от вирусов, но и как метод страховки на случай непредвиденного стечения обстоятельств или чьих-то (в том числе и собственных) действий. В особенности они важны для программистов, работающих на ассемблере, которые при отладке часто находятся буквально в шаге от разрушения файловой системы.

Поскольку дискеты являются в наших условиях дефицитом, то при архивировании информации ее целесообразно сжимать архиватором. Для дискет DS/DD наиболее подходящим форматом для записи архивов, по-видимому, является формат 800K, который достаточно надежен и позволяет вдвое уменьшить количество используемых дискет. Наиболее удобными архиваторами являются Fastback PLUS, Pkzip и Lha.

В условиях дефицита дискет при использовании Pkzip и Lha возникает дополнительная проблема оптимальной комбинации архивов на дискетах, чтобы более полно использовать емкость каждой дискеты. Для этой цели можно дополнительно упаковывать полученные архивы утилитой Backup MS DOS или более удобной и имеющей графический интерфейс утилитой PC-Backup из пакета PC Shell (рекомендуется использовать версии, начиная с 5.5). Если дискет не хватает для создания полной копии винчестера, то следует исключить из архивирования прежде всего большие пакеты (трансляторы, операционная система и т.д.), для которых имеются дистрибутивные копии.

В защиту "бумажной технологии"

"То, что вы храните достаточно долго, можно выбросить. Как только вы что-то выбросите, оно вам понадобится".

Из законов Мерфи

Наряду с архивом на дискетах следует вести часть архива на бумаге. Несмотря на отдельные заявления о наступлении эры "безбумажной технологии", роль этого старого доброго способа хранения информации сохраняется. Бумага все еще остается дешевым, надежным и удобным методом долговременного хранения текстовой информации, существенно превосходя по надежности магнитные носители, а по удобству анализа некоторых видов информации (например, дампов) — просмотр файлов на дисплее. Кроме того, наличие рабочего журнала является одним из показателей уровня квалификации программиста. По мнению автора, программист, не ведущий рабочий журнал, не может считаться высококвалифицированным. Систематическое ведение журнала позволяет быстрее и полнее осваивать новые системы, прогрессивные приемы работы и избегать уже допущенных ранее ошибок.

Необходимо систематически подшивать в специальную папку копии оглавлений, последние копии AUTOEXEC.BAT, CONFIG.SYS, список сбойных секторов винчестера (если таковые имеются), распечатки всех оглавлений диска, дампы бутсектора и FAT, замечания по работе машины, а также протоколы работы программы-ревизора. Кроме того, справочник по архиву дискет также целесообразно иметь в распечатанном виде, поскольку, если с

машиной что-то случится, считать его с винчестера может оказаться достаточно трудной задачей. Полезно, хотя и несколько трудоемко, вести отдельный архив распечаток исходных текстов разрабатываемых программ, в который подшивать все распечатки версий программ и другую аналогичную информацию. Наличие такого архива создает ряд удобств и является дополнительной гарантией сохранности информации.

Запомните параметры, хранящиеся в CMOS-памяти, пока еще не поздно

"Столб дыма уносит новости Богу..."

Теофиль Готье

Получив машину типа AT, сразу же запишите параметры CMOS, установленные с помощью процедуры SETUP. Для этого достаточно нажать комбинацию клавиш Ctrl-Alt-Esc. При этом на экран выдается таблица параметров, записанных в CMOS-памяти, из которых наиболее важным является тип установленного винчестера. Эта таблица невелика, и ее содержимое легко переписать на обычную самоклеящуюся этикетку для дискеты, которую необходимо сразу же прикрепить к лицевой стороне корпуса компьютера. После этого обязательно распечатайте содержимое CMOS на принтере. Это проще всего сделать с помощью утилиты SysInfo, из версии 5-й утилит П.Нортона. Один экземпляр распечатки рекомендуется наклеить на папку с планом восстановления винчестера (см. ниже), а другой — на последнюю страницу инструкции к данной ЭВМ. Кроме того, необходимо записать содержимое CMOS в файл с помощью программы DiskTool из 5-й версии утилит П.Нортона, CMOSer (СП 3-4) или SaveCMOS А.Водяника (СП 2-3). Для некоторых типов BIOS содержимое отдельных байтов CMOS не выдается на экран, однако важно для правильной работы машины.

Эти меры связаны с тем, что рано или поздно элемент, обеспечивающий питание CMOS-памяти, выйдет из строя. Кроме того, известно несколько троянских программ, которые при запуске портят CMOS. Иногда содержимое CMOS уничтожается из-за ошибки в "нормальной" программе. Хотя элемент питания рассчитан на несколько лет, опыт показывает, что средняя продолжительность жизни CMOS обычно не превышает нескольких месяцев. Если содержимое CMOS потеряно, то при отсутствии точных данных о типе установленного винчестера возникает ряд очень неприятных проблем, когда значение некоторых параметров приходится устанавливать экспериментально. Это особенно трудно, когда на машине установлен нестандартный (например, трехдюймовый) винчестер.

Переписывая программы, различайте эталонную и рабочую копию

Дистрибутивные эталонные версии рекомендуется хранить отдельно в архивированном виде. Если дисковод обеспечивает формат 720K, то на одну дискету обычно входит три архивных "образа" 360K дискет. Современные версии архиваторов (Pkzip 1.10, Lha 2.12, Arj 2.00) позволяют рекурсивно сворачивать подкаталоги, тем самым делая рассматриваемый вид хранения более привлекательным. При работе с Norton Commander рекомендуется определить для файлов с расширениями .ZIP, .ARC, .ARJ и .LZH вызов архиватора в режиме выдачи на экран справки с архива или вызов диалоговой оболочки для соответствующего архиватора (Shez, NARC и др.).

Передавая программы, копируйте дистрибутивные, а не рабочие копии. В нынешних условиях это долг вежливости по отношению к тому, кому переписывается программное обеспечение. Храните справки с дистрибутивной копии для сравнения. Для экономии дискет (особенно если дистрибутивная копия поставляется на 360K дискетах) удобно хранить дистрибутивные копии в виде файлов, содержащих образы дисков, созданных утилитой Dfcopy (СП 2-10), а затем сжатых подходящим архиватором (например, Lha, Ari, Charc и др.). При таком способе хранения на одну 800K дискету можно записать до четырех архивированных образов дискет.

Переписывая программы, старайтесь копировать дистрибутивные версии, а не рабочие копии, хранящиеся на винчестере. Обязательно отпечатайте справку с архива с контрольными суммами.

Очень полезно вести каталог используемых программ на dBase или какой-то аналогичной системе. За счет более точной информации о состоянии архива можно значительно уменьшить объем еженедельного архивирования и тем самым сэкономить время и силы.

Методика применения средств защиты

Методика применения средств защиты предполагает их наличие и желание ими пользоваться. К сожалению, часто можно констатировать отсутствие как первого, так и второго из этих условий. Спектр отношения пользователей к антивирусным программам колеблется от полного равнодушия до страстного коллекционирования. Однако наличие антивирусных программ является только необходимым условием. Важно не только иметь последние версии антивирусных программ, но и систематически ими пользоваться. К новым антивирусным средствам, полученным "обычным" путем, следует относиться с такой же осторожностью, как и ко всем остальным программам. Антивирусные средства, не снабженные средствами самоконтроля целостности, могут оказаться зараженными. Кроме того, изредка встречаются троянские версии антивирусных средств. Ранее уже упоминались троянские версии сторожа FluShot и полифага Aidstest.

Типичные ошибки

Как уже указывалось, самой грубой и распространенной ошибкой при использовании персональных компьютеров является отсутствие надлежащей системы архивирования информации. Никакие средства защиты не заменят хорошей организации ведения архивов.

Другой столь же грубой и столь же распространенной ошибкой является запуск только что полученной программы без ее предварительного анализа на зараженность и без установки максимального режима защиты винчестера с помощью ADM и запуска резидентного сторожа. Запуск программы является в современных условиях далеко не безопасной операцией, и рисковать содержимым винчестера из-за чрезмерного любопытства, наверное, не стоит. Следует также обратить внимание на ситуацию, характерную для школ и вузов. Поскольку у студентов обычно мало дискет, то им приходится запускать отдельные программы (например, игровые) с дискет своих товарищей. Эта ситуация особенно характерна для вузовских "залов персональных ЭВМ". При этом может произойти заражение одной из программ или бутсектора, если соответствующий компьютер оказался зараженным. Поэтому следует всегда защищать дискеты от записи, если они используются для считывания программ на нескольких компьютерах. Снимать защиту от записи стоит только на время, необходимое для обновления содержимого дискеты. Новые программы по возможности следует записывать на новые дискеты, не смешивая их сразу со старыми, проверенными программами.

При неправильном или неумелом использовании антивирусные программы могут сами в ряде случаев становиться источником проблем. Имеется несколько типичных ошибок при применении антивирусных средств. Наиболее грубой и распространенной из них является запуск антивирусных программ (чаще всего фагов) на зараженном резидентным вирусом компьютере. Конечно, сейчас создатели большинства качественных антивирусных средств предусматривают такую возможность и анализируют память компьютера перед началом работы, однако такая методика эффективна в основном против уже известных вирусов и может не сработать на каком-то новом. Поэтому следует особо подчеркнуть основной "гигиенический" принцип компьютерной вирусологии:

ВСЕ ДЕЙСТВИЯ ПО ИССЛЕДОВАНИЮ "ПОДОЗРИТЕЛЬНОГО" ИЛИ ЗАРАЖЕННОГО КОМПЬЮТЕРА СЛЕДУЕТ ВЫПОЛНЯТЬ ТОЛЬКО НА ПРЕДВАРИТЕЛЬНО ЗАГРУЖЕННОЙ С ЗАЩИЩЕННОЙ ОТ ЗАПИСИ ЭТАЛОННОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ И ИСПОЛЬЗУЯ ТОЛЬКО ПРОГРАММЫ, ХРАНЯЩИЕСЯ НА ЗАЩИЩЕННЫХ ОТ ЗАПИСИ ДИСКЕТАХ.

Выполнение действий по анализу и восстановлению файловой системы при наличии в памяти резидентного вируса является грубой ошибкой и может иметь катастрофические последствия. В частности, при этом могут быть заражены остальные, еще незараженные, программы. Например, при резидентном вирусе RCE-1800.DAV (Dark Avenger) запуск фага, не рассчитанного на данный вирус, приведет к заражению всех проверявшихся фагом загрузочных модулей, поскольку вирус RCE-1800.DAV перехватывает прерывание по открытию и чтению файлов и при работе фага будет заражать каждый проверяемый фагом файл.

Второй типичной ошибкой является выполнение перезагрузки системы при наличии "защелкнутой" дискеты в дисководе А. При этом BIOS делает попытку загрузиться именно с этой дискеты, а не с винчестера, и в результате, если дискета зара-

жена бутовым вирусом, происходит заражение винчестера.

Третьей распространенной ошибкой является запуск "батареи" фагов на всей файловой системе. Очевидно, что прогон десяти фагов, предназначенных для вируса C-648.VEN, приведет к нежелательным последствиям на компьютере, зараженном вирусом RCE-1800.DAV. Поэтому вначале следует выявить "подозрительные" файлы, переписать их на виртуальный диск или дискету и запускать все имеющиеся фаги и детекторы только на этой выборке. Если в указанной выборке имеются программы, сжатые Lzexe, их следует распаковать. В данном случае следует придерживаться принципа "лучше меньше, да лучше" и запускать средства защиты, предварительно просмотрев дампы "подозрительных" программ и протрассировав первые их команды отладчиком. В большинстве случаев это позволяет определить, что программы действительно заражены (если вирус не имеет самомодифицирующегося инсталлятора, то все или часть подозрительных программ при просмотре отладчиком имеют одинаковые начальные команды).

Четвертой типичной ошибкой является чрезмерная доверчивость к разработчикам антивирусных средств. Хотя разработкой антивирусных средств обычно занимаются высококвалифицированные программисты, не следует думать, что созданные ими программы безупречны. Как и всякие программы, они содержат ошибки, причем ситуация усугубляется тем, что те их части, которые относятся к самым новым вирусам и тем самым представляют наибольшую ценность, часто бывают написаны наспех, в условиях острейшего дефицита времени. Поскольку вирусы сильно различаются по степени своей распространенности, то отладка будет выполняться лишь для наиболее распространенных вирусов (т.е. примерно для 20% от общего количества "выкусываемых" вирусов). Для остальных шанс на исправление допущенной при написании фага ошибки невелик. Поэтому следует считать, что на вашей системе выполняется отладка этих новых частей, которая, как и всякая отладка, может иметь негативные последствия как для отдельных файлов, так и для файловой системы в целом. Если у вас нет свежего архива, то запуск любой антивирусной программы на всю файловую систему становится потенциально опасной операцией. Это относится прежде всего к фагам, выполняющим "хирургическое вмешательство" в программы. Известны случаи, когда фаг принимал один вирус за другой и все "вылеченные" программы оказывались неработоспособными.

Сканирующие антивирусные программы

Программы, в ходе своей работы просматривающие дерево каталогов, часто называют сканирующими. Для сканирующих антивирусных программ важным критерием является работа через BIOS для считывания управляющих блоков и другой контролируемой информации, а не использование для считывания функций операционной ситемы типа FindFirst, FindNext. Это требование связано с тем, что резидентный вирус может перехватить эти прерывания и "подсунуть" антивирусной программе "туфту" вместо записанной на диске информации.

Вторым общим критерием оценки сканирующих антивирусных программ является наличие самотестирования на заражение. Программы, не обладающие данным свойством, применять не рекомендуется.

Серьезной проблемой использования сканирующих программ является наличие целого ряда способов хранения информации на винчестере. В частности, важно понимать, что сканирующие программы не в состоянии выявить вирусы, хранящиеся в архивированных файлах. Для проверки такого рода файлов удобно запускать их через оболочку Shez, создав оболочку с именем Scan.exe с соответствующими параметрами, единственной функцией которой будет преобразование параметров и вызов соответствующей программы (Shez рассчитан только на запуск через него полидетектора Scan). Другим подводным камнем является существование динамически разархивируемого формата EXE-файлов (наиболее популярным является формат Lzexe, хотя он не является единственно используемым). Если зараженный файл был сжат этим архиватором, сканирующая программа не в состоянии определить его зараженность без динамически выполняемой распаковки. Поэтому на этапе входного контроля рекомендуется распаковывать файлы, предварительно упакованные с помощью Lzexe.

Сканирующие программы должны каким-то образом пытаться определить наличие в памяти резидентных вирусов, поскольку при резидентном вирусе процесс

сканирования может привести к заражению всех "проверенных" файлов. Причем, если заражение выполняется при закрытии файла, никакой диагностики выдано не будет. Эта проблема особенно актуальна для ревизоров, которые, по-видимому, должны иметь режим настройки на определенное состояние оперативной памяти (при запуске в AUTOEXEC. BAT).

Важным критерием оценки антивирусных программ является использование ими различного рода эвристических приемов, типа диагностирования значения 62 секунды в поле даты. Это повышает вероятность обнаружения новых вирусов.

Другой важный критерий — выдача более или менее подробного отчета. В настоящее время это является слабым местом для большинства программ. Например, для фага такой отчет должен включать, помимо имени файла и типа заражения, хотя бы длину файла до и после выкусывания. Кроме того, в случае обнаружения каких-то аномалий фаг должен выдавать соответствующую информацию и предупреждающие сообщения, а не "резать молча".

Общими критериями оценки сканирующих антивирусных программ являются:

самотестирование на заражение;

возможность управления областью поиска (глобальный по всем дискам, по одному диску, в поддереве, в одном каталоге, в одном файле);

управление суффиксами обрабатываемых файлов;

качество интерфейса (избыточный интерфейс с "лишними окнами" и навязчивым музыкальным сопровождением так же плох, как и недостаточный, типа реализованного в полидетекторе Scan);

качество диагностических сообщений;

качество помощи, если таковая предусмотрена;

качество параметризации;

качество документации;

возможность обработки файлов с атрибутами HIDDEN;

качество выдаваемого протокола;

размер в K;

скорость поиска;

оригинальность оформления (видео и звуковое сопровождение).

Ревизоры

Программы-ревизоры относятся к самым надежным средствам защиты от вирусов и должны входить в арсенал каждого пользователя. Ревизоры являются единственным средством, позволяющим следить за целостностью системных файлов и изменениями в используемых каталогах. Следует отметить, что получаемая с помощью ревизоров информация существенно облегчает ориентировку в лабиринте каталогов и "нововведениях" среди трансляторов и используемых утилит. Поэтому их нельзя рассматривать только в контексте защиты от вирусов — в настоящее время они должны быть рабочим инструментом каждого программиста.

Существуют два основных типа программ-ревизоров: пакетные (например, ADinf Д.Мостового, DLI В.Герасимова и др.) и резидентные. В данном разделе мы рассмотрим пакетные ревизоры. В связи с распространенностью стелс-вирусов, современные пакетные ревизоры обычно сканируют файловую систему, не используя прерывания 21 (операций файловой системы MS DOS). Ревизоры, использующие при работе прерывание 21 или в документации к которым этот вопрос не оговорен, использовать не рекомендуется. Это, в частности, относится к учебным программам, публикуемым в популярных учебниках по MS DOS (например, [Фигурнов 90] и [Фигурнов 90а]).

Пакетные ревизоры рекомендуется запускать по меньшей мере раз в день, перед началом первого сеанса работы с ЭВМ. Для этой цели их рекомендуется располагать в качестве первой или второй программы, вызываемой в AUTOEXEC. BAT. Если ревизор обладает способностью сканирования MBR и бутсектора, то его можно ставить первым. Если нет, то перед его вызовом рекомендуется поставить вызов программы, обеспечивающей контроль указанных блоков (AVB или SysTest).

Использование пакетных ревизоров особенно важно при работе на "персональных ЭВМ коллективного пользования", которые в СССР сейчас явно преобладают. В этих условиях необходимо, чтобы ревизор создавал отдельный файл с контрольными суммами, который можно было бы записать на дискету или в собственный каталог, а затем перед началом следующего сеанса работы выявить произошедшие изменения. Такое использование ревизоров должно сочетаться с "тотальной" проверкой целостности файлов, которую целесообразно проводить централизованно, не реже

одного раза в месяц, причем протоколы проверки целесообразно печатать и сохранять в специальной папке.

Следует отметить, что для контроля отдельных "подозрительных" или "странно ведущих себя" файлов можно использовать сравнение с дистрибутивной копией (если, конечно, заведомо известно, что это именно дистрибутивная копия). Это прежде всего относится к компонентам MS DOS, трансляторам, командным оболочкам. Сравнение (только перегрузившись с эталонной дискеты) можно выполнить с помощью обычных программ сравнения файлов, например входящие в MS DOS программы FC и COMP.

Из других качеств пакетного ревизора, которые могут служить критерием оценки его качества при выборе, отметим следующие:

возможность записи результатов ревизии в отдельный файл или распределения по проведенным файлам в виде специальной маркировки;

возможность сохранять первые байты программы;

качество алгоритма подсчета контрольной суммы;

возможность выдачи стандартной контрольной суммы (соответствующей выдаваемой архиваторами Pkzip, Lha и др.);

диагностика аномалий в дате создания файла (например, 62 секунды, 13 месяцев, год из следующего столетия и т.д.);

возможность выдачи данных ревизии в виде отчета с указанием размера и даты создания первых байтов;

возможность маркировки файлов перед передачей на другой компьютер и последующего снятия маркера.

Детекторы

Детекторы, рассчитанные на конкретные вирусы, также можно рассматривать как специализированные программы-ревизоры, однако качество обеспечиваемого ими анализа вызывает сомнения и они должны контролироваться другими методами, в частности с помощью глобального контекстного поиска. Следует отметить, что наиболее удобны детекторы, обнаруживающие не один, а целый ряд распространенных вирусов (полидетекторы). Имеются два основных типа полидетекторов: с фиксированным набором сигнатур и с переменным набором.

Детекторы с фиксированным набором сигнатур в общем случае эффективнее полидетекторов с переменным набором. Обычно такие детекторы являются составной частью полифага. Однако имеется и "чистый" полидетектор — Scan фирмы McAfee Associates (США). Текущая (на момент написания данной работы) версия полидетектора Scan детектирует более двухсот вирусов и их разновидностей (имеется и резидентная версия, проверяющая файлы при загрузке — Scanres). Качество детектирования невысокое (имеется много ложных срабатываний). Большинство используемых данным полидетектором сигнатур приведено в прил. (см. [Безруков 91]).

Среди полидетекторов, входящих в полифаги, следует отметить детектор, встроенный в полифаг TNTVirus. В отличие от полифага, являющегося коммерческим продуктом, полидетектор входит в распространяемую бесплатно демонстрационную версию. Эта громоздкая (более 100К) программа имеет неплохой турбоинтерфейс и детектирует более ста вирусов. Качество детектирования следует оценить как весьма среднее (в большинстве случаев используется обычный контекстный поиск). Многие из используемых сигнатур приведены в прил. (см. [Безруков 91]). За исключением интерфейса и количества сигнатур данный полидетектор уступает аналогичным отечественным программам по количеству ложных срабатываний и качеству распознавания наиболее распространенных в нашей стране вирусов. Из полидетекторов, встроенных в отечественные полифаги, наиболее интересен режим детектирования, обеспечиваемый полифагом SOS Е.Н.Сусликова и полифагом AV И.Сысоева. Последний обнаруживает порядка 40 вирусов, являясь при этом самой маленькой (менее 20К) и быстрой программой такого рода. Как уже указывалось, программы этого типа представляют наибольший интерес как средство входного контроля нового программного обеспечения, в особенности поступающего без контрольных сумм.

Второй тип полидетекторов более интересен, поскольку фактически представляет собой системные программы общего применения, которые можно использовать не только для поиска вирусов, но и во всех случаях, когда нужно найти все файлы, содержащие хотя бы одну из заданной группы текстовых строк (ключевых слов). Набор строк для поиска обыч-

но задается в виде специального файла. Этот тип полидетекторов наиболее полезен при обнаружении какого-то нового, еще неизвестного, вируса. Первое, что нужно сделать в этом случае, — определить сигнатуру для поиска. Надежнее всего использовать для этой цели трассировку зараженной программы с помощью отладчика. Определив сигнатуру, можно быстро выявить все зараженные программы и тем самым прекратить дальнейшее размножение вируса. Имеется ряд программ этого типа (VL, Virscan). Например, программа VL (см. приложение) обеспечивает поиск в поддереве или файле до 50 строк длиной до 15 символов. Строки задаются пользователем в текстовом или 16-ричном формате. Дамп программы, в которой найдена строка, можно просмотреть на экране. Программа NeaDet, написанная И.В.Суворовым, позволяет использовать в качестве входных данных приведенные в [Безруков 91] таблицы и специальный алгоритм быстрого поиска строк. Дамп программы, в которой найдена строка, можно просмотреть на экране.

Если попытаться перечислить критерии оценки качества детектора в порядке убывания их важности, то получится следующий список:

проверка оперативной памяти и нейтрализация резидентных частей вируса;

количество одновременно детектируемых вирусов;

диагностирование многократно зараженных разнотипными вирусами файлов;

степень параметризации, совместимость по параметрам со Scan;

удобство ввода новых сигнатур для поиска;

возможность визуального просмотра дампа найденных файлов;

использование эвристических приемов детектирования (диагностирование "подозрительных" переходов до 4K от конца файла, специальных последовательностей команд и др.);

наличие средств сокращения количества ложных срабатываний при поиске (комбинирование сигнатур, использование регулярных выражений, определение точки входа и др.);

операции с найденными файлами (удаление, копирование, переименование и т.д.)

диагностирование "спецслучаев" типа программ, сжатых Lzexe, Exepack, программ с внутренней сегментацией и др.

Первым критерием оценки качества детектора является наличие проверки оперативной памяти на сигнатуры вирусов. Дело в том, что, хотя детекторы не должны запускаться на машине, загруженной с винчестера (т.е. потенциально зараженной), полагаться на добросовестность пользователей было бы опрометчиво. Качественный детектор должен иметь режим выдачи протокола на принтер в виде отчета, а также режим просмотра дампа найденного файла на экране дисплея. Лучшие из детекторов, помимо поиска сигнатур, используют ряд эвристических приемов, позволяющих выявить потенциально опасные программы. К таким приемам относятся интерпретация первой команды в COM-файлах и определение расстояния от точки, в которую передается управление, до конца файла. В случае, если это расстояние меньше, скажем 4K (вообще порог срабатывания следует задавать как параметр), такую программу необходимо подвергнуть дополнительному анализу.

Следует иметь в виду, что сигнатуры, используемые в детекторах, часто являются весьма несовершенными, что приводит к многочисленным ложным срабатываниям. При этом качество выдаваемых детекторами диагностических сообщений обычно довольно низко, а их текст настолько непродуман, что вызывает ложную тревогу и различные недоразумения. Обычно чем более прост детектор, тем категоричнее выдаваемые им сообщения. Так, большинство детекторов, основанных на простом поиске в файле определенной, характерной для данного вируса строки (т.е. обладающие теми же возможностями диагностики, что и Norton Utilities или PC Tools), в случаях, когда она найдена, выдают "самоуверенное" сообщение типа:

Файл XXXX заражен вирусом ZZZZ.

На самом деле текст должен выглядеть гораздо скромнее, например:

На расстоянии YYYY от конца файла XXXX найдена строка, характерная для вируса ZZZZ.

В этом плане характерен пример весьма популярного в нашей стране полидетектора Scan фирмы McAfee Associates, который детектирует наибольшее число известных вирусов. Этот весьма низкокачественный, по сути, любительский детектор дает много ложных срабатываний, в частности для вирусов RC-1701 и Fu Manchu. Тем не менее пользователи упорно считают выдаваемую им диагностику "окончательным и не подлежащим обжалованию приговором". Автору как редактору бюллетеня "Софтпанорама" приходится отвечать на множество звонков, "сигнализирующих" о наличии вирусов в той или иной программе, включенной в очередной выпуск бюллетеня. На вопрос "Как это Вам удалось установить?" обычно следует стандартный ответ: "С помощью Scan". Поэтому при входном контроле программного обеспечения рекомендуется применять несколько детекторов

("батарею") и рассматривать выданные сообщения как результаты голосования. В спорных случаях следует провести визуальный анализ дампа с помощью таких средств, как Norton Commander, PC Shell или Norton Utilities.

Другой ошибкой, характерной для детекторов, является пропуск зараженных вирусом программ (детектор обычно ориентирован на конкретный набор характерных для вируса строк и не может учитывать возможность появления новых штаммов). Например, тот же Scan пропускает ряд распространяющихся в нашей стране вирусов. Поэтому выдаваемое детекторами в конце работы сообщение типа:

Нет зараженных файлов

следует рассматривать под тем же углом, что и предыдущее сообщение. Кроме того, пропуск зараженных программ детектором возможен из-за "непродуманной оптимизации". Например, ряд детекторов для повышения скорости работы сканируют не весь файл, а только его последние несколько блоков. Если вирус "аномально" сел в середину файла, он будет таким детектором пропущен.

Следует также отметить, что неэффективен запуск программ-детекторов для проверки архивированных файлов (т.е. файлов с расширениями .ZIP, .ARC, .ICE, .LZH и т.д.). Для проверки программ, находящихся в архивированном виде, необходимо предварительно их разархивировать или использовать специальную оболочку, автоматически разархивирующую каждый файл перед передачей детектору. В противном случае детектор не в состоянии проверить содержимое архива, поскольку соответствующие сигнатуры искажены в процессе сжатия информации.

Для проверки архивов с помощью Scan удобно запускать его из оболочки Shez (версии 5.5 и более поздние), которая позволяет автоматически разархивировать проверяемые файлы. Это означает, что совместимость со Scan по передаваемым параметрам обеспечивает важный и удобный режим работы. Тем самым такая совместимость становится важным критерием оценки качества детекторов (как, впрочем, и фагов).

Рассмотренные выше ошибки были характерны как для детекторов, так и для фагов, поскольку фаг обычно включает в себя детектор. Теперь перейдем к ошибкам, характерным только для фагов.

Использование Norton utilities и PC Tools как универсальных детекторов вирусов

Как уже указывалось, обеспечиваемая PC Tools и Norton Utilities возможность выполнения контекстного поиска как по отдельным файлам, так и по диску в целом служит полезным и надежным инструментом выявления зараженных файлов. В особенности полезна возможность выполнения глобального контекстного поиска по диску в целом. При правильном выборе строки для контекстного поиска этот способ, хотя и довольно медленный, но исключительно надежный метод определения всех зараженных вирусом файлов. Следует отметить, что Norton Utilities выполняет контекстный поиск примерно вдвое быстрее, чем PCTools.

Поиск текстовых сигнатур

При поиске Т-сигнатур бывает полезна программа TS из версии 4.5 пакета утилит П.Нортона. Она позволяет искать заданный текст в файле или по всему диску, например:

```
TS C:\*.COM vacsina /S /LOG
TS C:\*.EXE eddie /S /LOG
```

В программе можно использовать ряд ключей:

/LOG — печатать или выводить результаты в файл;

/S — просматривать также и подкаталоги;

/T — выводить только окончательные результаты;

/D — искать по всему диску (отменяет /S);

/E — искать по стертым файлам;

/CS — различать малые и большие буквы.

Фаги

Следует отметить, что программы-фаги, обеспечивающие возможность восстановления исходного состояния программы, зараженной вирусом, хотя и относятся к наиболее популярным типам антивирусных программ, но не являются основным средством защиты от вирусов. Наблюдаемая сейчас повсеместная погоня за последними версиями фагов не совсем оправдана. Основные усилия должны быть направлены на предупреждение заражения (грамм профилактики стоит килограмма лекарств).

Отметим, что программы, которые мы для краткости называем "фагами", по сути,

представляют собой комбинацию типа "детектор + фаг". Поэтому при их работе возможны как ошибки, связанные с несовершенством детектора, так и ошибки при "выкусывании" вируса из программы. Для фага неверное "выкусывание" вируса из зараженной программы ("больной умер на операционном столе") может быть обусловлено как ложным срабатыванием детектора, так и недостаточным учетом возможных вариантов заражения программы. При этом фаг уничтожает работоспособную программу (хотя с этим утверждением можно не соглашаться, но, по мнению автора, зараженная программа все же лучше, чем никакая). Поэтому при применении фагов для файловых вирусов целесообразно разделять процесс диагностирования и процесс "лечения".

Кроме того, распространяющиеся сейчас комплексные фаги на несколько вирусов (полифаги) менее удачны, чем полидетекторы, поскольку жесткая привязка фага к конкретному "встроенному" детектору делает его "заложником" качества последнего, а отсутствие параметров настройки на вирус — чувствительным к мутациям вируса, затрагивающим используемую сигнатуру. Единственным фагом, где была сделана попытка преодолеть этот недостаток, является полифаг Neatfag В.В.Пономаренко. В нем фаг на каждый вирус выполнен в виде отдельного загружаемого модуля, что позволяет добавлять модули, "выкусывающие" новые вирусы отдельно, без переделки уже имеющейся части фага. Однако возможность замены или добавления сигнатур в существующей версии Neatfag отсутствует.

Процесс дезактивации рекомендуется разделить на ряд этапов, с тем чтобы не повредить файловую систему во время ее выполнения. Можно рекомендовать следующие этапы указанного процесса:

загрузиться с защищенной от записи дискеты, используя "холодную" (кнопкой RESET или выключением питания), а не "теплую" (нажатием клавиш CTRL-ALT-DEL) перезагрузку;

найти хотя бы одну зараженную программу с помощью батареи детекторов;

проверить правильность идентификации типа вируса, визуально просмотрев дамп зараженной программы;

составить список зараженных программ и распечатать этот список;

выгрузить зараженные программы на дискету и обработать их фагом;

проанализировать результаты выкусывания;

проверить работоспособность "леченных" программ и выгрузить их.

Если COMMAND.COM заражен, то используйте его размер и дамп для определения типа вируса. Если нет, то поиск зараженной программы можно выполнить разными способами, но обязательно перегрузившись с защищенной дискеты. Если используется программа-ревизор и ведется архив каталогов файловой системы, то целесообразно воспользоваться им. Если нет, то проще всего использовать рекомендованную выше батарею полидетекторов (только перегрузившись с защищенной дискеты!), с помощью которой, возможно, удастся определить зараженные или хотя бы "подозрительные" файлы (некоторые детекторы используют для этой цели эвристические приемы).

Составьте список зараженных программ с помощью детектора и проверьте его полноту глобальным контекстным поиском (см. ниже). Все зараженные программы выгрузите на дискету, сделайте ее копию и экспериментируйте только на ней. Если имеется возможность, то выгрузите из архива оригинальные копии программ на другую дискету или на винчестер. После прогона фага опять распечатайте оглавление, сравните длины зараженного и "вылеченного" файлов и визуально просмотрите дампы программ. Для тех программ, данные о длинах которых сохранились (например, в базе данных ревизора) или оригинальные копии которых имеются в архиве, проверьте, правильно ли восстановлена длина. Если такой возможности нет, то предварительно проверьте работоспособность "леченной" программы и только после этого сгрузите ее обратно на винчестер. Помните, что фаг может испортить программу. И наконец, с помощью детектора и глобального контекстного поиска проверьте полученные результаты: не осталось ли на диске зараженных программ.

Следует отметить, что предложенные шаги в полном объеме необходимы только при работе с новым, еще недостаточно изученным вирусом или "самодельным" фагом (например, изготовленным по методике, описанной во второй части данной работы). Для хорошо изученных вирусов, для которых существуют достаточно надежные

и проверенные фаги, большинство из этих шагов можно опустить.

Помимо критериев, приведенных выше для полидетекторов, полифаги можно оценивать по следующим критериям:

количество обрабатываемых вирусов;

обработка выполняемых файлов, сжатых Lzexe;

обработка многократно зараженных файлов;

возможность управления временем создания файла (например, сброс и установка 62 с для заданных файлов);

самовосстановление при заражении вирусами (включая неизвестные);

лечение многократно зараженных вирусом программ (например, RCE-1813);

выдача предупреждений при обнаружении файлов аномальной структуры или нестандартных случаев заражения (типа заражения FoxBase вирусом RCE-1813).

В настоящее время большинство полифагов ориентировано на фиксированный набор вирусов и неэффективно против всех остальных типов. Поэтому качество фага прежде всего связано с количеством вирусов, которые он обрабатывает, и правильностью его работы. Наряду с этим показателем немаловажное значение имеют удобство интерфейса и выдача более или менее подробного отчета. Такой отчет должен позволять контролировать результаты "лечения" и включать, помимо имени файла и типа заражения, хотя бы длину файла до и после "выкусывания". Кроме того, обнаружив какие-либо аномалии, фаг должен выдавать предупреждающие сообщения, а не "резать лишь бы резать". Наличие качественной документации также является несомненным достоинством, но, к сожалению, среди некоммерческих программ встречается редко.

Как уже указывалось, по выполняемым действиям фаги, особенно сканирующие всю файловую структуру, являются потенциально опасными программами. Например, некоторые фаги проверяют тип файла не по его первым байтам, а по расширению, что ведет к плачевным результатам при лечении EXE-программ с расширением .COM или COM-программ с расширением .EXE. Поэтому применять новый, неопробованный фаг следует, только приняв необходимые меры предосторожности, в частности, предварительно отделив зараженные программы от остальных и сняв справки до и после лечения. Кроме того, встречаются фаги, зараженные вирусами (часто другого типа), или даже вирусы, замаскированные под фаги (на одной из первых дискет с антивирусными программами, распространявшейся по стране, имелись две программы — AntI86 и AntI87, которые представляли собой вирус C-648 с добавленными к нему для камуфляжа сообщениями).

Подобно любой другой часто используемой программе, фаг может содержать троянскую компоненту. Например, если рассматривать пакет антивирусных программ В.Бончева, то, учитывая тот факт, что им распространялась дискета с текстами вирусов (хотя хочется надеяться, что это была "ошибка молодости"), нет никакой гарантии, что в очередной версии один или несколько фагов данного пакета не окажутся троянскими, например, будут лечить от одного вируса и заражать другим. В частности, один из вирусов, разработанных в институте ВМЕИ им.В.И.Ленина (В. Бончев называет эту серию вирусов TP-вирусами), модифицирует вирус "Итальянский попрыгунчик", и его несложно выдать за резидентный фаг. Поэтому относиться к программам Бончева, учитывая нездоровый интерес, проявляемый к его имени со стороны технокрысы Dark Avenger, нужно с осторожностью. Это, впрочем, относится к любой антивирусной программе, полученной из неизвестного или сомнительного источника. Например, на Западе в одной из сетей распространялась троянская программа, которая имитировала заставку FluShot3, представляясь ее новой версией — FluShot4. При запуске этой программы на экране появлялась заставка с запросом: "Желаете ли вы инсталлировать программу в систему?" Независимо от сделанного пользователем ответа программа уничтожала системные блоки винчестера и разрушала нулевой сектор на всех доступных дискетах.

Резидентные программы

Большинство алгоритмов, используемых в пакетных разновидностях рассмотренных типов антивирусных программ, можно реализовать и в резидентном варианте. И такие попытки делались и делаются. Вместе с тем резидентные программы имеют свою специфику. Главным критерием для них является объем занимаемой оперативной памяти и степень наводимых помех пользователю и интерференция с другими резидентными программами.

Что касается объема занимаемой памяти, то, по мнению автора, антивирусные резидентные программы, занимающие более 10% имеющейся оперативной памяти, "слишком много на себя берут".

Дисковые драйверы и кэши

Некоторые дисковые драйверы и кэши, помимо выполнения базисных функций, имеют дополнительные возможности, обеспечивающие повышенный уровень защиты от вирусов. К таким средствам прежде всего относится возможность присваивания логическим разделам винчестера статуса READ ONLY, что является абсолютно необходимым средством в современной обстановке.

Резидентные ревизоры

В отличие от своих пакетных "коллег" резидентные ревизоры выполняют подсчет контрольных сумм "на лету", т.е. при загрузке программ на выполнение. Несколько устаревший сторож FluShot Plus очень полезен тем, что включает резидентный ревизор, позволяющий "на лету" подсчитывать контрольную сумму для загружаемых файлов. К сожалению, отдельного резидентного ревизора, обеспечивающего подсчет контрольной суммы "на лету", перед передачей файлу управления, пока нет.

Резидентные вакцины

"Притворяясь, будто мы попали в расставленную нам ловушку, мы проявляем поистине утонченную хитрость, потому что обмануть человека легче всего тогда, когда он хочет обмануть нас".

Франсуа де Ларошфуко

Как известно, вакцинирование домашних животных и человека, открытое Л.Пастером, является одним из фундаментальных открытий XX века. Учитывая аналогию между компьютерными и биологическими вирусами, следовало бы ожидать соответствующей эффективности "кибернетических вакцин", которые изменяют среду функционирования вируса таким образом, что он теряет способность к размножению. Однако на сегодняшний день этот тип антивирусных программ особого распространения не получил.

В настоящее время используются два основных типа резидентных вакцин: основанные на инактивированном теле вируса и основанные на имитации действий, обеспечивающих положительный ответ на проверку вирусом в запускаемой программе инсталлированной в памяти копии. Инактивированная вакцина может быть получена из тела вируса гораздо быстрее, чем написан соответствующий фаг. Поэтому такой тип вакцин можно рекомендовать как временную меру после обнаружения какого-то нового вируса. Недостатком такого подхода является необходимость рабочего знания языка ассемблера. Первая вакцина, основанная на инактивированном вирусе, была разработана Л.И.Обуховым для вируса RCE-1813 (СП 1-2) и применялась в Киеве при борьбе с эпидемией указанного вируса. Наиболее мощная поливакцина была разработана студентом КИИГА В.В.Пономаренко (СП 2-7,3-2) и получила название Neatvac. Существующая версия Neatvac обеспечивает защиту от более чем десятка резидентных вирусов и особенно удобна для вузовских машинных залов, где чаще обычного приходится сталкиваться с зараженными программами. В то же время вакцины, как и любые дополнительные резидентные программы, не лишены побочных эффектов, которые могут быть связаны с перехватом прерываний, используемых, помимо вируса, и какой-нибудь "нормальной" резидентной программой.

Если говорить о критериях оценки поливакцин (на самом деле выбора здесь практически нет), то стоит отметить следующие критерии:

количество обрабатываемых вирусов;

самотестирование на заражение;

нейтрализация резидентных вирусов или блокирование запуска на зараженной машине;

диагностирование зараженной программы;

степень наводимых помех при работе.

Резидентные сторожа

Современные программы-сторожа — резидентные программы, выявляющие запуск зараженной программы и/или блокирующие предпринимаемые вирусом несанкционированные действия, такие, как IWP, MVT, Check21 и др., эффективны против большинства известных файловых вирусов. Устаревшими, но все еще распространенными сторожами являются MaceVaccine и ANTI4US2. Возможности

этих программ уже не соответствуют уровню написания современных файловых вирусов, наличие их в памяти создает значительные помехи при работе, поэтому постоянно запускать их через AUTOEXEC.BAT не рекомендуется. Вместе с тем использование этих сторожей обязательно при первых запусках нового программного обеспечения, когда возможно не только заражение вирусом, но и немедленное срабатывание троянской компоненты.

Следует подчеркнуть, что наиболее эффективно кратковременное применение этих сторожей: непрерывные ответы на запросы, выдаваемые сторожами, не только снижают эффективность работы, но и подрывают саму обеспечиваемую ими защиту (это относится прежде всего к устаревшим сторожам типа FluShot Plus, MaceVaccine, ANTI4US2). Частая выдача запросов на разрешение тех или иных действий неизбежно приводит к тому, что пользователь начинает отвечать на них механически, тем самым сводя на нет обеспечиваемую ими степень защиты. Современные сторожа должны иметь "таблицу свойств" программы, позволяющую блокировать выдачу запросов на разрешение тех или иных операций от соответствующих программ. Например, если программа FORMAT пытается выполнять форматирование диска C, то запрос на разрешение этого действия следует блокировать.

Степень обеспечиваемой сторожами защиты не стоит переоценивать. Некоторые типы вирусов обходят сторожей, непосредственно обращаясь к BIOS, или используют сплайсинг (врезку) для получения управления по прерыванию 21. Поэтому их применение должно сочетаться с применением других средств защиты, в частности ревизоров. Теоретически вирус может обойти любой метод блокирования записи, за исключением аппаратных (из упомянутых выше резидентных сторожей только IWP может работать в сочетании со специальной аппаратной платой — Port Watch Card). Однако практически сложность вируса ограничена, и большинство технокрыс предпочитают "быстрые и грязные" методы, основанные на недокументированных особенностях MS DOS. Это создает хорошие предпосылки создания достаточно универсальных сторожей, создающих минимум помех при работе. Следует отметить, что сторожа могут интерферировать с резидентными программами, а также вызывать срабатывание фагов, проверяющих содержимое оперативной памяти. Последние часто принимают сторожа за вирусы.

Если говорить о критериях оценки сторожей, то наиболее важными представляются следующие:

степень помех при работе;

блокирование несанкционированных попыток записи на диск (включая форматирование);

блокирование изменений в BOOT и MBR;

блокирование несанкционированной постановки программы в резидент;

наличие средств ведения протокола;

наличие звукового сигнала и управление им.

Отдельные приемы защиты

"Привычка — вторая натура".

Латинская пословица

В данный раздел включены некоторые приемы, которые, хотя и носят вспомогательный характер, в то же время достаточно важны для того, чтобы предпринять специальные меры по их выделению из массы приводимого материала.

Регулярно оптимизируйте винчестер

Как уже указывалось, периодически следует оптимизировать расположение файлов на винчестере с помощью утилиты SpeeDisk Нортона или другой аналогичной утилиты. Эту операцию целесообразно проводить не реже раза в месяц, сразу после выгрузки содержимого винчестра на дискеты (создания главного архива). В процессе оптимизации файлы можно расположить на диске таким образом, чтобы наиболее часто используемые находились ближе к началу диска. Для этой цели можно скорректировать поле даты таким образом, чтобы у наиболее часто используемых файлов дата создания была меньше, чем у используемых редко, а затем задать режим упорядочения файлов по дате. Помимо этого, SpeeDisk позволяет также задать порядок расположения каталогов и имена нескольких наиболее часто используемых файлов.

Ежедневно перед окончанием работы следует проводить "уборку винчестера" — дефрагментацию созданных файлов. После дефрагментации все файлы занимают последовательные группы кластеров, что существенно облегчает их восстановление

даже в случае тяжелых повреждений управляющих блоков.

Прятать новые версии антивирусных программ просто невыгодно

*"Что ты спрятал, то — пропало.
Что ты отдал, то — твое".*

Ш.Руставели

Получив новую, более эффективную антивирусную программу, некоторые не стремятся передать ее другим пользователям, рассматривая ее наличие как некоторое преимущество. Ошибочность политики "примитивного эгоизма" в случае антивирусных программ состоит в том, что, передав программу всем своим знакомым, вы как бы создаете дополнительную зону защиты, на которой тот или иной вирус может быть обнаружен и изолирован еще до попадания на вашу ЭВМ. Поэтому бескорыстная передача новых версий антивирусных программ представляет, по сути, политику "разумного эгоизма": за ваше более безопасное положение вы отдаете чужие, доставшиеся вам бесплатно программы да еще и получаете причитающуюся вам долю уважения за кажущееся бескорыстие этих действий.

Нормальное состояние дискеты — защищенное от записи

К существенному конструктивному дефекту 5-дюймовых дискет относится необходимость заклейки выреза клейкой фольгой для защиты от записи. При этом фольга, как и сами дискеты, является дефицитом. Тем не менее рекомендуется считывать информацию с дискеты, в особенности на "чужих" машинах, только с защищенных от записи дискет. Вообще нормальное состояние дискеты — "заклеенное", и защита должна сниматься только в случае записи на нее информации. В условиях дефицита наклеек из фольги для этой цели можно использовать "самодельные", состоящие из полоски фольги, наклеенной на прозрачную липкую ленту (SCOTCH) или темную изоленту. В случае, когда у вас на машине не оказалось наклейки, а вам нужно защитить дискету от записи, можно сложить пополам полоску бумаги так, чтобы она закрывала соответствующую прорезь, и аккуратно вставить ее в дисковод вместе с дискетой.

Как работать на зараженном файловым вирусом компьютере при отсутствии вакцины

Иногда необходимо работать на компьютере, который постоянно инфицируется любителями компьютерных игр или по каким-то другим причинам. В этом случае можно избежать заражения используемых программ путем создания искусственной мишени для вируса. Поскольку подавляющее большинство файловых вирусов заражает программу при ее запуске, можно обмануть вирус двумя основными способами.

В этом случае все выполняемые программы следует хранить в архивированном виде, а для запуска на выполнение использовать простой BAT-файл, первым параметром для которого яляется имя исполняемой программы и содержащий последовательность шагов, в которых программа сначала разархивируется на виртуальный диск, затем переименовывается, выполняется и удаляется. При отсутствии достаточного количества оперативной памяти для организации виртуального диска требуемого размера можно использовать один из разделов винчестера, хотя это несколько замедляет работу. Преимущество этого способа (если держать архиватор на виртуальном диске) — в экономии места на диске, а недостаток — увеличение времени поиска программ при загрузке, связанное с просмотром архива. Автор разработал последний способ после одного неудачного эксперимента с вирусом RCE-1800, когда "вырвавшийся на свободу" вирус заразил несколько десятков файлов на винчестере (никакими специальными ЭВМ для экспериментов автор не располагает, поэтому все эксперименты проводятся "с риском для винчестера" на обычном персональном компьютере коллективного пользования). Вместе с тем данный способ оказался достаточно удачным и с тех пор широко используется автором для экономии места на винчестере.

Особенно полезен данный способ для мелких, сравнительно редко применяемых программ, если на используемой машине установлен винчестер размером 20М или меньше. В этом случае на винчестере создается рабочий каталог (например, WORK), в который выполняется разархивирование. Этот каталог включается в PATH перед каталогом BAT, а в Norton Commander (или другую используемую оболочку) включается команда очистки этого каталога. Поскольку из каталога WORK разархивированная программа не

удаляется, то дополнительное время на разархивацию тратится только при первом обращении к программе. Конечно, следует предусмотреть соответствующий BAT-файл для запуска программы (в простейшем случае это может быть BAT-файл RUN, которому в качестве первого параметра передается имя выполняемой программы).

Для "монстрообразных" программ (например, программ, написанных на Clipper'е) очень удобно использовать архиватор Lzexe (см. СП 2-9). Например, программа PC Tools занимает на диске около 200K, половину из которых можно сэкономить, сжав ее с помощью Lzexe.

Вместе с тем следует отдавать себе отчет, что, если архивации или сжатию подвергается зараженная программа, определить ее зараженность после этого большинство имеющихся полидетекторов и фагов не смогут. Таким образом, при ее запуске компьютер будет заражаться вирусом.

При хранении антивирусных программ на винчестере используйте архивирование

При хранении антивирусных программ в виде специального каталога на винчестере желательно свернуть их в архив, а перед использованием разархивировать на виртуальный диск или в тот же каталог, а затем удалять. Это позволяет избежать заражения антивирусных программ, не обладающих средствами самотестирования на зараженность, новыми типами вируса, которые, естественно, ими не детектируются (в лучшем случае может быть выдано предупреждающее сообщение).

Использование дрозофил для определения типа заражения и местонахождения спрятанных байтов

В ряде случаев приходится "лечить" файлы вручную, используя только редактор двоичных файлов (например, Red). В этом случае первостепенное значение имеет выяснение расположения "спрятанных" вирусом байтов. В частности, для COM-файлов в большинстве случаев достаточно восстановить первые три байта, чтобы дезактивировать вирус. При наличии некоторых навыков, после проверки правильности работы дезактивированной программы можно легко удалить тело вируса редактором.

При определении местонахождения спрятанных байтов удобно использовать "неразборчивость" вирусов, которые не проверяют, какие файлы им "подсовывают для заражения". Поэтому вместо настоящего можно создать файл, состоящий из одинаковых символов, и заразить его изучаемым вирусом. Поскольку в простейшем случае этот файл неисполняемый, то в случае резидентного вируса, заражающего запускаемые на выполнение программы, после заражения MS DOS зависнет и вам придется перегрузиться. Однако зараженный файл сохранится и окажет неоценимую помощь при анализе. Обычно достаточно нескольких экспериментов, чтобы определить местонахождение "спрятанных байтов". Это позволяет выяснить их местонахождение без дисассемблирования.

Немного зная ассемблер, можно легко сделать и исполняемый макет, состоящий из требуемого количества команд nop (однобайтовая команда с кодом 90h) и выхода с помощью int 20 или int 21-4C. Такие макеты будем называть дрозофилами. Некоторые вирусы заражают только файлы, начинающиеся с команды перехода. В таких случаях в дрозофиле необходимо поставить первой команду jmp. Для создания таких дрозофил удобно использовать программу Debug, входящую в состав MS DOS. Техника работы с этой програмой подробно описана во всех учебниках по языку Ассемблера для IBM PC.

МЕТОДИКА ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ

"Ничего не потеряно, пока не потеряно все".

Пословица

Необходимо отметить, что даже в достаточно тяжелых случаях, восстановление поврежденной информации чаще всего возможно (по крайней мере частичное), однако требует достаточно высокой квалификации. Именно в этот момент "вступают в игру" архивированные системные блоки, наличие которых на дискете позволяет существенно облегчить восстановление.

Наряду со свежими архивными копиями системных блоков в такой ситуации важное значение имеет наличие системных программистов, способных оценить характер и объем повреждения, а также умеющих выполнить восстановление при разрушенных или отформатированных сис-

темных блоках или других массивных повреждениях файловой системы. При отсутствии собственных системных программистов представляется оправданным приглашение их со стороны. Конечно, степень усилий во многом зависит от ценности потерянной информации. В силу ограниченности пространственного объема остановимся лишь на наиболее общих принципах организации восстановления информации.

Создайте и отработайте план восстановления винчестера

> *"Кто приготовился к бою, тот его наполовину выиграл".*
>
> М.Сервантес

Встреча с каким-нибудь коварным компьютерным вирусом может и не состояться. Но огорчаться не стоит. Экстремальных ситуаций в программировании хоть отбавляй, и место вируса наверняка не окажется вакантным. Поэтому вопрос не в том, потеряете ли вы данные, записанные на винчестер, а лишь в том, когда это произойдет. Следовательно, уже сейчас стоит подумать над вопросом о том, как реагировать на это неприятное событие, которое обычно случается в самый неподходящий момент. Результаты ваших раздумий следует оформить в виде папки с документами ("горячая папка") и коробки с дискетами ("горячая коробка"), которые вместе мы будем называть планом восстановления винчестера.

Первая компонента плана — "горячая папка" — должна содержать всю информацию, необходимую для восстановления винчестера. Для машин типа AT на лицевую сторону обложки следует наклеить распечатку содержимого CMOS-памяти, полученного с помощью программы SysInfo, входящей в 5-ю версию утилит Нортона или с помощью другой подходящей утилиты. На обратную сторону папки следует наклеить распечатку Partition Table всех логических дисков. Ее можно получить с помощью Norton Utilities. На обороте папки карандашом удобно записывать даты создания архивов логических дисков и имена файлов с протоколами архивирования. В самой папке будем хранить распечатку последних версий AUTOEXEC. BAT и CONFIG.SYS, а также тетрадь, в которой записаны необходимые шаги по восстановлению основных каталогов и комментарии к ним (с указанием встретившихся трудностей и "топких" мест). В папке также желательно хранить распечатку каталогов всех логических дисков винчестера и каталогов всех дискет "горячей коробки".

"Горячая коробка" должна состоять из лучших дискет, которыми вы располагаете (желательно 1.2 М, если на машине установлен соответствующий дисковод). Эти дискеты должны быть проверены и не содержать сбойных треков. Примерный состав "горячей коробки":

1. Дискета со стартовой операционной системой. Если вы используете Disk Manager или ADM, то дискета со стартовой операционной системой должна включать в CONFIG.SYS соответствующий драйвер. Если на компьютере установлен дисковод 1.2 М, то стартовая дискета должна быть именно 1.2 М, а не 360 К, как это часто бывает. При загрузке операционной системы со стартовой дискеты необходимо предусмотреть организацию электронного диска размером в 200 К при обьеме оперативной памяти в 640 К, или 384 К при обьеме оперативной памяти в 1 М. В процессе загрузки на этот электронный диск должен переписываться командный процессор и Norton Commander, с тем чтобы не приходилось держать на каждой дискете копию командного процессора. Все EXE-файлы на стартовой дискете целесообразно сжать архиватором Lzexe. В случае дискеты 360 К полезно преобразовать в EXE-формат и сжать COM-файлы. Ввиду особой важности целесообразно иметь две идентичные копии стартовой дискеты.

2. Дискеты с утилитами. На эти дискеты рекомендуется записать Norton Utilities версии 5 и PC Tools. Если дискеты имеют объем меньший 1.2 М, то все нужные программы можно разместить на двух дискетах.

3. Дискета с программами разметки винчестера и установки используемого дискового драйвера. На данной дискете целесообразно разместить соответствующие программы (ADM, Disk Manager, SpeedStore и др.) и текстовый файл с планом разбиения винчестера.

4. Дискета с резервными копиями управляющих блоков. Эта дискета должна иметь подкаталоги C, D, E и т.д., в каждом из которых следует хранить управляющие блоки, относящиеся к данному диску. Файлы с резервными копиями управляющих блоков проще всего сделать с помощью программы DiskEdit версии 5 утилит Нортона. При этом MBR можно записать в файл

MBR.BIN, бутсектор в файл BOOT.BIN, а затем сделать их распечатки. Программа DiskTool версии 5 утилит Нортона позволяет создать объединенные дампы MBR и бутсекторов всех логических дисков, которые следует записать в корневой каталог данной дискеты. Она также выполняет дамп CMOS. Помимо указанных статических управляющих блоков, которые достаточно записать на дискету один раз, необходимо периодически записывать на эту дискету дампы FAT и главного каталога. Для этой цели удобно использовать файлы, создаваемые программой Image на диске. Их следует скопировать в соответствующий подкаталог дискеты с помощью Norton Commander или другой аналогичной оболочки.

5. Fastback Plus и протоколы выгрузки для каждого логического диска.

6. Программы тестирования оборудования.

7. Электронный справочник TechHelp фирмы.

План восстановления винчестера должен быть реально отработан хотя бы один раз. Для этой цели целесообразно устроить "учебную тревогу" — после полной выгрузки информации на дискеты стереть вручную, скажем, главный каталог винчестера, предварительно создав его копию на диске в помощью программы Image из 5-й версии утилит Нортона и записав на дискету программу восстановления (Unformat). Наверняка уже на начальных шагах восстановления обнаружится ряд серьезных проблем, преодаление которых приведет к существенному уточнению первоначального плана. Зато в кризисной ситуации "полетевшего винчестера" можно будет действовать более спокойно и уверенно, зная, что все нужные программы записаны на дискеты и архив успешно восстанавливался.

Если что-то случилось — избегайте поспешных действий

"Утро вечера мудренее".

Пословица

При обнаружении вируса и в особенности при уничтожении им какой-то информации очень важно не предпринимать поспешных действий и прежде всего не запускать никаких программ с винчестера и не записывать на диск новой информации. Рекомендуется сначала "остановиться, оглядеться, перегрузиться с дискеты", поскольку при этом существенно повышаются шансы того, что уничтоженная информация может быть восстановлена в полном объеме. Даже если диск отформатирован, содержащаяся на нем информация может быть в ряде случаев восстановлена. При обнаружении каких-то повреждений информации или файловой структуры запуск любых программ, записывающих информацию на винчестер, является грубой ошибкой, обычно существенно увеличивающей количество потерянной информации.

Поспешное восстановление обычно приводит не только к потере части файлов, но и к повторному заражению. Характерным примером непродуманных поспешных действий является реакция некоторых пользователей на ложное сообщение сторожа FluShot Plus о попытке модификации CMOS ("экзотический" тип памяти для машин типа AT). Вместо выяснения ситуации, которая может быть редкой и связанной с типом памяти, назначение которой далеко не все отчетливо себе представляют, такие пользователи "доверчиво" отвечают на запрос FluShot — восстановить (правильный ответ — игнорировать), что приводит к затиранию CMOS-памяти без помощи вируса. Вместе с тем "экзотичность" ситуации делает вполне оправданным телефонный звонок специалисту, на который достаточно потратить 5-10 мин, что позволяет в большинстве случаев избежать неприятных последствий. Другим примером является использование Norton Disk Doctor версии 4.5 при восстановлении информации на винчестре. В ряде случаев, особенно при использовании дисковых драйверов, использующих нестандартный формат MBR, его применение может давать непредвиденные результаты. Кроме того, если указанной программой восстанавливается сектор, содержащий каталог, то, хотя его содержимое переносится в другой кластер, ссылка в родительском каталоге продолжает указывать на старый кластер, что может вызывать эффект "двоящегося каталога". Эти недостатки устранены в версии 5.0 утилит Нортона.

Не рекомендуется начинать восстановление винчестера "сразу после события" или во второй половине дня. Поскольку часть информации так или иначе пропала и потери времени неизбежны, лучше всего прекратить работу в этот день и заняться чем-нибудь другим. Не

исключено, что за это время в голову придет какая-нибудь удачная идея, которая позволит существенно уменьшить обьем работы по восстановлению.

Советы по восстановлению информации

Прежде чем начать восстановление информации на диске, восстановите CMOS, MBR и бутсектор. Используя файлы, записанные в базе данных восстановления с помощью программы DiskTool 5-й версии утилит Нортона, восстановите указанные блоки. MBR и бутсектор относятся к статическим управляющим блокам, и внесение изменений в них фактически возможно только при переразметке винчестера. CMOS имеет динамические поля (дата и время) однако их значение некритично. Этот прием обеспечивает заведомо правильное значение типа винчестера в CMOS, границы логических дисков и параметры разметки (количество секторов в кластере и и другая информация из бутсектора). При этом файлы, из которых вы производите восстановление, должны принадлежать данному винчестеру и компьютеру, иначе можно наломать дров. Затем следует проверить правильность восстановления CMOS, MBR и бутсектора визуально.

Если компьютер загружается с дискеты, но винчестер не читается, то сначала оцените объем повреждений. Первое, что нужно сделать в данном случае — это просмотреть управляющие блоки и определить степень их повреждения. Если блоки читаются и информация в них не слишком искажена, то соответствующие сектора диска следует записать в виде файлов на дискету с помощью Norton Utilities и распечатать дамп утилитой TDump или какой-нибудь аналогичной. Помимо визуального сравнения, рекомендуется получить протокол различий имеющегося и эталонного MBR, бутсектора, FAT и корневого каталога. Это можно сделать с помощью утилиты FC, входящей в MS DOS. Затем следует запустить Norton Disk Doctor II и записать выдаваемую им диагностику. К выдаваемым сообщениям следует относиться критично. Никаких действий по исправлению до подтверждения "диагноза" по другим источникам разрешать не следует.

Перед началом восстановления выполните съем информации на дискеты с помощью DiskEdit. Теперь можно более уверенно работать, не боясь окончательно испортить информацию. При наличии более мощного компьютера, восстановление информации удобнее проводить на нем, записав выгруженные сектора в виде файла, а затем создав дополнительный каталог, восстанавливать цепочки в FAT. Конечно, для этой цели нужно выделить отдельный рабочий диск или выгрузить один из имеющихся разделов винчестера, поскольку операции с FAT лучше проводить на "чистом" диске.

Если компьютер не загружается с дискеты, переставьте винчестер на другой компьютер с подходящим контроллером. Если вышел из строя какой-то блок компьютера, то винчестер можно переставить на другой компьютер и прочитать информацию там. Если это не представляется возможным, то лучше снять винчестер с данной машины и переставить его на время восстановления на более мощный компьютер.

При большом объеме работ по восстановлению доукомплектуйте компьютер еще одним винчестером или дисководом. Если предстоит большая и сложная работа по восстановлению информации, то нельзя пытаться сделать ее "наскоком". Нужно обязательно провести подготовительную работу. В частности, на время восстановления полезно доукомплектовать компьютер вторым винчестером (желательно аналогичного типа) и дисководом 1.2 М. В наших условиях в качестве дополнительного винчестера подойдет на 20 М с какой-нибудь вышедшей из строя Мазовии или Правца. Это существенно упрощает вызов необходимых программ и хранение промежуточной информации во время восстановления.

НЕКОТОРЫЕ ПРИЕМЫ РАБОТЫ НА КОМПЬЮТЕРЕ С ОДНИМ ДИСКОВОДОМ

Каждый, кому приходилось восстанавливать винчестер на компьютере, имеющем один дисковод, знает, что большая половина усилий уходит не на восстановление, а на преодоление неудобств, связанных с ограниченностью конфигурации. Первое, что стоит сделать в таких условиях, это предусмотреть перенесение командного процессора и некоторых утилит на электронный диск. При размере электронного диска в 384К, как это имеет место на большинстве поставляемых в нашу страну АТ, на электронный диск можно записать, помимо командного процессора, архиватор

Pkzip и Norton Commander. При этом еще остается возможность распаковывать небольшие файлы на электронный диск. При отсутствии электронного диска даже копирование отдельного файла с дискеты на дискету представляет определенную проблему. Для этой цели следует задавать команду:
COPY A:\COMMAND.COM B:

Несмотря на то что диск B физически отсутствует, операционная система правильно выполнит команду, позволяя после считывания файла вынуть исходную дискету и вставить новую. Таким же образом следует поступать при копировании больших файлов. Правда, в этом случае удобнее пользоваться утилитой Xcopy.

ОРГАНИЗАЦИОННЫЕ И ПРАВОВЫЕ МЕТОДЫ ЗАЩИТЫ ОТ ВИРУСОВ

Организационные и правовые методы защиты от вирусов тесно связаны с экономическими проблемами. Действительно, решение купить ту или иную систему защиты от вирусов является альтернативой, скажем, покупке нового компилятора или партии дискет. Например, неразумно затратить, скажем, 500 руб. на защиту информации, цена восстановления которой не превышает 50 руб. Вообще говоря, затраты на приобретение и установку средств защиты можно оценивать как своего рода страховочные платежи.

Некоторые организационные меры защиты

"Как всякий человек на своем месте, как подчиненные его самого, Лужин ругал высшее начальство, считая, что там сидят дураки, бюрократы, самодуры, которые отдают приказы, совершенно не считаясь с их практической выполнимостью".

В.Войнович "Жизнь и необычайные приключения солдата Ивана Чонкина"

Хотя в данной работе рассматриваются в основном технические аспекты защиты от компьютерных вирусов, представляется целесообразным кратко остановиться и на организационных методах, поскольку они, по сути, являются одной из составных частей защиты наряду с техническими и программными методами. Как уже указывалось, независимо от того, насколько хорошо разработаны программные средства защиты, их эффективность во многих случаях непосредственно зависит от правильности действий пользователя, действий, в которых возможны не только ошибки, но и "несознательность" или даже злой умысел. Например, если один из сотрудников регулярно запускает где-то переписанные игровые программы на компьютере с винчестером, то шансы на то, что поставленная программная защита не сможет предотвратить заражение, безусловно отличны от нуля.

Среди спектра организационных мер отметим следующие, представляющиеся автору наиболее важными: общее административное регулирование доступа, включая систему паролей и сегментирование зон доступа; обучение персонала; обеспечение физической безопасности компьютера и магнитных носителей; выработку правил архивирования; определение файлов, хранимых в шифрованном виде.

Общее административное регулирование доступа

Общее административное регулирование доступа должно обеспечивать приемлемую степень защиты от использования компьютеров с ценными данными случайными лицами. Если человек оставляет на улице автомобиль с незапертыми дверцами и вставленным ключом зажигания, то, если его угонят, определенная доля вины будет лежать на этом человеке. Ситуация с компьютерами аналогична. Помимо опасности заражения вирусами, незаконное копирование или модификация конфиденциальной информации может нанести значительный вред организации, не обеспечившей приемлемый уровень контроля за контингентом пользователей соответствующего компьютера.

Если говорить о системе паролей, обеспечиваемых рядом систем, например DR DOS, то с организационной точки зрения важно, чтобы пароли были достаточно длинными, с целью предотвращения их случайного угадывания. К простому и в то же время достаточно хорошо зарекомендовавшему себя методу получения таких паролей относится комбинирование пароля из двух хорошо знакомых слов. Например, пароли "Коля" и "1950" каждый в отдельности весьма уязвимы, однако их комбинация типа К1о9л5я0 уже гораздо труднее дешифруется и не так легко может быть запомнена путем подглядывания "через плечо". Кроме того, пароли дол-

жны периодически меняться, причем для пользователей, которые не желают делать это добровольно, сответствующую "услугу" должен оказывать системный программист. Случаи, когда пользователи по нескольку лет применяют один и тот же пароль, безусловно, должны быть исключены.

Обучение персонала

В наших условиях обучение часто выполняется халатно и не обеспечивает требуемого уровня знаний. Это, в частности, препятствует распространению ревизоров, поскольку пользователи игнорируют выдаваемые им сообщения. Поэтому реальным критерием обученности персонала является его способность правильно действовать в условиях, максимально приближенных к реальности. Такие ситуации следует создавать в виде учебных тревог и отрабатывать на специальном компьютере, не содержащем ценных данных.

Опасность бесконтрольного запуска электронных игр

Как уже указывалось выше, сотрудник, запускающий на компьютере с винчестером новую игру, недавно полученную у приятеля, безусловно подвергает компьютер определенному риску, степень которого, конечно, зависит от уровня его квалификации, наличия резидентных средств защиты, а также применения им различных средств тестирования нового программного обеспечения на наличие компьютерных вирусов. Применительно к этой достаточно типичной ситуации важным организационным моментом является предоставление персоналу, имеющему "склонность" использовать в свободное время различные игры (электронщики, персонал, эксплуатирующий какую-нибудь систему и т.д.) специального компьютера, не содержащего сколь-нибудь ценные данные. Такое решение значительно эффективнее запретительных мер, которые, как показывает практика, легко обходятся. При продуманной организации можно добиться того, чтобы, с одной стороны, персонал не чувствовал себя ущемленным, а с другой, ценная информация не подвергалась бы опасности искажения или уничтожения.

В этой связи необходимо отметить, что большинство прикладных и системных программистов болезненно переживают любые ограничения в доступе к компьютеру. Поэтому наряду с "отходным вариантом" в виде дополнительного компьютера должна быть проведена достаточно квалифицированная и дипломатичная разъяснительная работа, с тем чтобы сотрудники осознали уровень реальной опасности и согласились поддерживать необходимые меры защиты.

Разграничение доступа не панацея

Представим себе гипотетическую ситуацию, когда один из пользователей, обладающий минимальными правами доступа (например, для которого винчестер доступен только в режиме чтения), столкнулся с зараженной игрой, которая стала работать несколько "странно". Он, естественно, обращается за помощью к системному программисту, который, будучи перегруженным, сначала решает посмотреть, что происходит непосредственно на машине. Для этого он входит в систему со своим паролем (и соответственно максимальным уровнем доступа) и "для пробы" один раз запускает эту игру. Не требуется объяснять, к какому результату приведет такой "пробный" запуск. Вместо системного программиста в роли "троянского коня" может выступить практически любой более компетентный (и обладающий соответственно большими правами доступа) пользователь, к которому обратятся с той же просьбой.

Физическая безопасность компьютеров

Имеет смысл устанавливать наиболее ценные персональные компьютеры на металлические столы со специальными закрываемыми нишами для блоков или снимаемым металлическим колпаком. Кстати, установка компьютера на прочном металлическом столе полезна и с точки зрения предотвращения повреждения винчестера от случайных толчков и колебаний. Не случайно Роджер Олфорт в статье "Десять советов по эксплуатации накопителей на жестких магнитных дисках" (Мир ПК, 1990 № 3) пишет:

"... накопители на жестких дисках не любят грубого обращения. Даже такие, на первый взгляд, безобидные факторы, как книга, брошенная на стол, или случайные толчки стола проходящими коллегами, могут привести к тому, что

головки чтения/записи накопителя чиркнут по поверхности дисков и испортят данные. Чтобы свести к минимуму вероятность подобной ситуации, рекомендуется устанавливать компьютер на прочный стол. Лично я работаю на стальном столе, прочном, как танк".

Учитывая, что стоимость изготовления такого стола существенно ниже стоимости компьютера, данная рекомендация заслуживает внимания. Да и простое прикрепление системного блока к столу, на котором он установлен, в наших условиях совсем не помешает.

Аналогичные замечания относятся к дискетам. Дискеты с ценной информацией следует хранить в сейфе, а не в ящике письменного стола. Конфиденциальная информация должна шифроваться. В рамках расематриваемой темы это прежде всего относится к зараженным программам, образцам вирусов, а также материалам их дизассемблирования и реконструкции.

Организация срочной антивирусной помощи, "горячая линия"

Важной организиционной мерой как в масштабах отдельной организации (особенно крупной), так и в масштабах отдельной территории (города, области, республики) является наличие эффективных каналов распространения информации о новых вирусах и антивирусных программах, а также наличие какой-то формы оперативного консультирования пользователей по возникающим у них проблемам. Создание такого рода инфраструктуры не только позволяет минимизировать время "свободного" распространения вируса, но и создать систему предупреждения пользователей о появившемся вирусе и эффективных для данного вируса мерах профилактики заражения. В рамках отдельной организации эту функцию может выполнять отдельное лицо.

В этом плане одно из оптимальных решений — это организация своего рода "антивирусной скорой помощи", которая бы оперативно реагировала на все случаи заражения компьютеров вирусами. Подобно обычной медицинской скорой помощи, ее антивирусная разновидность должна осуществляться бесплатно или за чисто символическую плату. Именно эта форма услуг может и должна финансироваться государством, а не дорогостоящие ведомственные "прожекты", кончающиеся "нулеводческими" отчетами, компилируемыми из "подручного фонда" бесплатно распространяемых сведений, включая данную работу.

Юридические методы защиты

"Oleynikoz S., 1990"

Строка, содержащаяся в вирусе RC-600

"Вы не глядите, что Серега все кивает, он соображает, все понимает! Что молчит — так это от волненья, от осознанья и просветленья. Не запирайте, люди!.."

В.Высоцкий
"Милицейский протокол"

Антропоморфизм в терминологии ("заражение", "вирус") не должен заслонять суть дела: вирусы — это специальный метод саботажа с помощью преднамеренно созданных для этой цели программ. Хотя вопросы юридической ответственности лиц, занимающихся созданием и распространением вирусов, достаточно сложные, они успешно решаются в США и западноевропейских странах. Уголовная ответственность за создание и распространение компьютерных вирусов принята сейчас в большинстве западных стран. При этом можно выделить следующие действия, подпадающие под существующий уголовный и административный кодекс: изменение данных (удаление, вставка, замена или перестановка данных, осуществляемая без ведома владельца); компьютерный саботаж (препятствование важной для предприятия или лица деятельности); повреждение имущества (если поврежденным имуществом является непосредственно ЭВМ или ее компонента); шпионаж (обеспечение доступа для себя или для другого лица к данным, не предназначенным для использования этими лицами, и доступ к которым защищен специальным образом); фальсификация документов (в случае, если вирус изменяет данные, предназначенные для доказательства того или иного статуса, или права данного лица, или группы лиц). При этом наказание может нести не только непосредственный разработчик, но и исполнители и соучастники. При наличии последних можно говорить о преступной группе.

Если задаться вопросом о мотивации разработки компьютерных вирусов, то

становится очевидной неоднородность разработчиков. Можно выделить группы разработчиков вирусов:

- *технопаты.* Технопаты — та же разновидность вандалов, которая при отсутствии компьютеров "разрисовывает" кабины лифтов, стены подъездов и т.д. Описание этого вида психических отклонений можно найти в любом учебнике психиатрии, и мы подробнее на них останавливаться не будем;

- *студенты.* В большинстве вузов доступ к компьютерам не контролируется, что дает возможность студентам, а иногда и их друзьям из школьников старших классов или учащихся техникумов заниматься чем угодно, включая написанием вирусов. Написание вируса не требует особой подготовки, помимо знакомства с операционной системой и языком Ассемблера, и представляет собой вполне доступную задачу, по меньшей мере для части студентов младших курсов. На конференции ANTIVIR-90 в качестве шуточного метода профилактики было предложено включить лабораторные работы по написанию вирусов в учебный план и устроить дифференцированный зачет. Автор этого предложения основывался на том, что в условиях советских вузов это один из самых надежных способов навсегда отбить охоту заниматься каким-то предметом;

- *обиженные сотрудники.* Некоторые троянские программы создавались специально как средство мести по отношению к "плохому начальнику". Готовность программистов отомстить за обиду с помощью логических бомб уже была продемонстрирована в нескольких случаях. Поэтому такая возможность должна учитываться администраторами при увольнении сотрудников, в особенности для невротических личностей;

- *террористы, преступники, политически мотивированные группы.* Компьютерные вирусы могут быть использованы как средство шантажа или пропаганды. К этой группе можно отнести упоминавшиеся ранее случаи вируса в базе данных по СПИД (Aids Information Trojans), бутового вируса Stoned (с лозунгом легализовать марихуану) и др. К этой же группе следует отнести разработчиков средств защиты от несанкционированного копирования, предусматривающих различного рода "карательные меры", при запуске программы на компьютере, отличном от того, на котором выполнялась инсталляция. Вирусы могут использоваться как орудие шантажа или средство дискредитации. В этой связи следует упомянуть о таком опасном преступлении, как "вирусный рэкет". Одна из разновидностей последнего — это сознательное заражение программного обеспечения, поставляемого вместе с компьютером, с целью извлечения дополнительной прибыли в виде платы за последующую дезинфекцию. На Западе отмечались случаи вирусного шантажа, когда неизвестное лицо по телефону сообщает об угрозе "взрыва" установленной вирусной "мины", способной разрушить ценную информацию. Как и в случае с шантажистами, сообщающими об установке мины в самолет, даже в случае, если угроза оказывается ложной, персонал теряет массу времени на поиски и проверку программного обеспечения;

- *военная разведка и спецслужбы.* По некоторым данным, вирусы рассматриваются различными спецслужбами как одно из возможных средств борьбы с противником. Действительно, нетрудно представить себе последствия попадания разрушительного вируса в компьютерную систему, имеющую стратегическое и тактическое значение. Вместе с тем результаты соответствующих исследований, если они ведутся, будут строго засекречены и вероятность попадания разработанных для этих целей вирусов на гражданские компьютерные системы ничтожна.

Таким образом, если на одном конце спектра находится мелкий пакостник, который создаст вирус с целью продемонстрировать "городу и миру" какой-нибудь "сногсшибательный", с его точки зрения, эффект, то на другом конце спектра находится уголовник, использующий вирус для шантажа пользователей. В любом случае выявление и попытка привлечь к судебной ответственности разработчиков компьютерных вирусов относится к важной форме борьбы с распространением компьютерных вирусов.

Разработка компьютерных вирусов не является уголовно наказуемым деянием. Однако когда разработанный вирус (в виде исходного кода или зараженной программы) был опубликован (помещение программы в BBS или электронный бюллетень рассматривается как опубликование), распространен или передан третьим лицам с согласия разработчика или без оного, возникает административная или уголовная ответственность в зависимо-

сти от ущерба, нанесенного деятельностью созданного вируса. При этом опубликование или распространение исходного кода вируса может квалифицироваться как подстрекательство (публичное или тайное воздействие на другое лицо с целью принятия им решений об осуществлении уголовно наказуемых действий) и вести к уголовной ответственности по соответствующей статье. При этом несущественно наличие каких-либо рекомендаций по его использованию, включая отрицательные рекомендации типа "ни в коем случае не делайте...".

Учитывая наблюдающийся сейчас рост преступности, нет никаких сомнений в том, что в нашей стране будет быстро расширяться и та ее часть, которая прямо или косвенно связана с компьютерами, т. е. компьютерная преступность. Уже сейчас можно говорить о советском вирусном взрыве, аналогичном болгарскому. Попадание разработанных в нашей стране вирусов на Запад приведут к созданию стереотипа, который будет препятствовать закупкам любого разработанного в нашей стране программного обеспечения. Поэтому фактический ущерб, наносимый разработчиками вируса, значительно превышает тот, который можно подсчитать исходя из непосредственно нанесенного вирусом ущерба. В то же время шансы на принятие законодательных мер в этом направлении в обозримом будущем невелики. Это связано прежде всего с тем, что в нашей стране еще не решены основные вопросы авторских прав на программное обеспечение.

Правда, некоторая надежда остается на имеющиеся статьи Уголовного кодекса. В частности, в Уголовном кодексе УССР имеется статья 90 "Неосторожное уничтожение или повреждение государственного или общественного имущества". В случае, если в результате заражения вирусом программного обеспечения, управляющего некоторым оборудованием, последнее получило повреждение, то возбуждение уголовного дела против разработчика вируса представляется возможным и рамках действующего законодательства. Вторая возможность вытекает из определения хулиганства как умышленных действий, грубо нарушающих общественный порядок и которые выражают явное неуважение к обществу. Поэтому разработка и распространение вируса, особенно в случае выдачи вирусом каких-либо сообщений типа "XXX — скотина" и т.д., может квалифицироваться по статье 206 "Хулиганство", предполагающей максимальное наказание в виде тюремного заключения сроком на один год. Часть II данной статьи ("Злостное хулиганство") предполагает максимальное наказание в виде тюремного заключения сроком до пяти лет. Кстати, прецедент имеется: именно по этой статье был осужден программист, заложивший логическую бомбу, вызвавшую остановку главного конвейра Горьковского автозавода. Например, исполнение вирусами группы "Гимн" Гимна СССР после уничтожения информации на винчестере может быть квалифицировано как злостное хулиганство.

Что касается возмещения убытков, то в Гражданском кодексе УССР имеется статья 440 "Общие основания ответственности за причинение вреда", которая гласит:

"Вред, причиненный личности или имуществу гражданина, а также вред, причиненный организации, подлежит возмещению в полном объеме лицом, причинившем вред.

Причинивший вред освобождается от его возмещения, если докажет, что вред причинен не по его вине".

Некоторые судебные процессы над кракерами и разработчиками вирусов

Имеющиеся сведения почти целиком основаны на американских данных. Сведения о судебных процессах в Европе на момент написания книги отсутствовали. Сведения приводятся в хронологическом порядке. Все описанные ниже процессы велись на основе принятого в 1986 г. американского закона о компьютерных преступлениях (1986 U.S. Computer Fraud and Abuse Act).

Процесс Зинна. В феврале 1989 г. 17-летний уроженец Чикаго Герберт Зинн был осужден окружным судом Северного района шт. Иллинойс на девятимесячное заключение в тюрьме для малолетних преступников. Он обвинен в незаконном доступе к компьютерам фирмы AT&T в Напервилле (шт. Иллинойс), компьютерам НАТО в Бирлингтоне и на базе военно-воздушных сил в шт. Джорджия. По данным обвинения, между июнем и сентябрем 1987 г. Зинн похитил программное обеспечение на сумму порядка 1,2 млн. долларов, включая очень ценные программы в области искусственного интеллекта и разработ-

ки компьютеров. Он был выявлен служащими компании AT & T, обнаружившими его телефонный номер и сообщения в одной из BBS. Это было первое осуждение по упомянутому выше закону от 1986 г.

Процесс Митника. В марте 1989 г. 25-летний Кевин Давид Митник был осужден к году тюремного заключения и трехлетнему испытательному сроку за кражу программы защиты от несанкционированного доступа, разработанную американской фирмой DEC. Стоимость разработки составила порядка 1 млн. долларов. Компания затратила более 100 тыс. долларов (преимущественно машинного времени) на расследование факта кражи. Митник также обвинялся в незаконном использовании 16 чужих кодов для уклонения от оплаты междугородных телефонных переговоров и в проникновении в компьютер университета Лидза (Leeds) в Великобритании. Однако в ходе слушаний прокурор согласился снять эти обвинения. Интересно отметить, что в приговоре предусматривалось шестимесячное лечение Митника в реабилитационном центре "с целью избавления его от навязчивого пристрастия к компьютерам".

Процесс Морриса. Как уже указывалось, 23-летний Роберт Тарран Моррис младший, бывший аспирант Корнельского университета оштрафован на 10 тыс. долларов, а также осужден на три года условно и 400 часов общественных работ. Моррис является автором вируса, поразившего в ноябре 1988 г. американскую национальную сеть Internet. Слушания по делу Морриса проходили в окружном суде штата Нью-Йорк с 22 января по 4 мая 1989 г. Приговор, вынесенный 4 мая 1989 г., основан на упомянутом выше законе от 1986 г. Осуждение основано на факте несанкционированного доступа Морриса к компьютерам и нанесении ущерба в 150 тыс. долларов государственной сети компьютеров. Основная часть этого ущерба связана с потерями машинного времени и времени, затраченного персоналом на восстановление операций сети. Адвокат Морриса заявил, что сумма ущерба раздута заинтересованными организациями.



ЛИТЕРАТУРА

[Абакумов89] Абакумов А.А., Абрамов С.М. и др. Правдивая история о жизни и смерти одного вируса // Наука в СССР. — 1989. — N 4. — С.83-87.

[Абрамов89] Абрамов С.М., Пименов С.П. и др. Компьютерный вирус // Микропроцессорные средства и системы. — 1989 — N 2. — С.22-24.

[Агасандян90] Агасандян Г. Не вреди ближнему своему // Компьютер. - 1990. - N 1. — С.47-49.

[АгеевА89] Агеев А.С. "Компьютерные вирусы" и безопасность информации // Зарубежная радиоэлектроника. - 1989. - N 12. — С.71-75.

[АгеевК90] Агеев К., Цал М. Чудеса в нашем "зоопарке" // Файл - 1990. — С.61-65.

[Батурин90] Батурин Ю.М. "Компьютерное преступление" — что за термином ? В кн: Право и информатика. — М.: МГУ, 1990. — С.89-99.

[Безруков88] Безруков Н.Н. Эвристические методы повышения качества дизассемблирования // Программирование. - 1988. - N 4. — С.81-93.

[Безруков89] Безруков Н.Н. Классификация компьютерных вирусов и средства защиты от них В кн: Эксплуатация программного обеспечения вычислительных систем реального времени, построенных на базе микро- и мини-ЭВМ. — Киев: КИИГА, 1989. — С.3-21.

[Безруков90а] Безруков Н.Н. Классификация компьютерных вирусов в МС ДОС // Программирование. - 1990. - N 3. — С.3-22.

[Безруков90б] Безруков Н.Н. Классификация вирусов: попытка стандартизации // Интеркомпьютер. - 1990. - N 2. — С.37-39; N 3. — С.38-47.

[Безруков90в] Безруков Н.Н. Классификация компьютерных вирусов MS DOS и методы защиты от них. — М.: СП "Информэйшн Компьютер Энтерпрайз", 1990. — 48 с.

[Безруков91] Безруков Н.Н. Компьютерная вирусология. — Киев: Украинская советская энциклопедия, 1991. — 416 с.

[Беляева91] Беляева С. "Мне было интересно попробовать". Интервью с человеком, заразившим Москву компьютерным вирусом // Комсомольская правда. - 1991. - 31 января.

[Бончев89а] Бончев В. Истината за компютърните вируси // Компютър за вас, 1989, г.5, N 1-2. — С.5-6.

[Бончев89б] Бончев В. Още за компютърните вируси // Компютър за вас, 1989, г.5, N 3-4. — С.8-15.

[Бончев89в] Бончев В. В търсене на универсалната ваксина // Компютър за вас, 1989, г.5, N 5-6. — С.8-12.

[Бончев89г] Бончев В. Компютърните вируси: епидемията продължава // Компютър за вас. - 1989. - г.5, N 7-8. — С.2-6.

[Бончев89д] Бончев В. Лихайският вирус // Компютър за вас. - 1989. - г.5. - N 910. — С.4-5,49.

[Бончев90а] Бончев В.В. Компютърните вируси и методи за борба с тях // АИТиАС. - 1990. - г.6. - N 1. — С.37-41.

[Бончев90б] Бончев В. Новите вируси в България // Компютър за вас. - 1990. - г.6. - N 1-2. — С.2-5.

[Бончев90в] Бончев В. Играта загрубя: за вируса Eddie и неговия злополучен автор // Компютър за вас. - 1990. - г.6. - N 3-4. — С.9-10.

[Бончев90г] Бончев В. Вирусна поща: отговори на найчестите въпроси // Компютър за вас. - 1990. - г.6. - N 3-4. — С.11-14.

[Бончев90д] Бончев В. Борбата с компютърните вируси чрез световните електронни мрежи // Компютър за вас. - 1990. - г.6. - N 7-8. — С.2-4.

[Бончев90е] Бончев В. Новото на вирусния фронт // Компютър за вас. - 1990. - г.6. - N 7-8. — С.5-7; N 9-10. — С.6-9.

[Бончев90ж] Бончев В. Вирусни новини // Компютър за вас. - 1990. - г.6. - N 9-10. — С.9-11.

[Внук90] Внук П. 10 антивирусных заповедей // Компьютер. - 1990. - N 1. — С.49.

[Герасимов89] Герасимов Ю.В. Программы — вирусы персональных компьютеров // Инф. бюллетень Центра ПЭВМ МАП. - 1989. - N 4. — С.12-25.

[Гутников90] Гутников А. Компьютерный вирус // Радио. - 1990. - N 7. — С.40-41.

[Горбунов90] Горбунов Н. Вирус — мститель // Студенческий меридиан. - 1990. - N 1. — С.21-22.

[Давыдовский90] Давыдовский А.И., Максимов В.А. Введение в защиту информации // Интеркомпьютер. - 1990. - N 3. — С.17-20.

[Декларация89] Декларация "Принципы развития индустрии программирования на основе защиты интеллектуальной собственности" // Соц. индустрия. - 1989. - N 161. — С.2.

[Дзержинский90] Дзержинский Ф.Я. Комментарий о вирусах и компьютерном пиратстве // Программирование. - 1990. - N 3. — С.23-24.

[Диев89] Диев С.И. Защита информации в персональных компьютерах // Зарубежная радиоэлектроника. - 1989. - N 12. — С.57-59.

[Зуев90] Зуев К.А. Компьютер и общество. — М.: Политиздат, 1990. — 315 с.

[Известия90] "Черный мститель" неуловим // Известия. - 1990. - 4 января.

[ИНО88] Способы совершения компьютерных преступлений (обзор) // Информатика и право: теория и практика буржуазных государств. — М., 1988. — С.76-103. — (Сер. Информация, наука, общество).

[Кадлоф90] Кадлоф А. Вирусы // Компьютер. - 1990. - N 1. — С.44-47.

[Карасик89а] Карасик И.Ш. К вопросу о компьютерных вирусах // Мир ПК. - 1989. - N 3. — С.127-131.

[Карасик89б] Карасик И.Ш. Несколько слов о компьютерных вирусах // Интеркомпьютер. - 1989. - N 1. — С.14-15.

[Карасик89в] Карасик И.Ш. Типология вирусов // Интеркомпьютер. - 1989. - N 2. — С.14-15.

[Карасик90а] Карасик И.Ш. Анатомия и физиология вирусов // Интеркомпьютер. - 1990. - N 1. — С.39-47.

[Карасик90б] Карасик И.Ш. Классификация антивирусных программ // Интеркомпьютер. - 1990. - N 2. — С.40-45.

[Карлитин89] Карлитин Л.Е. Доктор Ватсон берет реванш у Шерлока Холмса // Наука в СССР. - 1989. - N 4. — С.80-82.

[КВ884] Вируси в паметта // Компютър за вас. - 1988. - г.4. - N 4-5. — С.12-13.

[КВ891] Ваксината ANTI // Компютър за вас. - 1989. - г.5. - N 1-2. — С.7.

[Комягин90] Комягин В.Б. Антивирусная программа VP — Virus protector // Интеркомпьютер. - 1990. - N5. — С.42-46.

[Куренков89] Куренков С.Д. Компьютерные вирусы и методы борьбы с ними // Международный симпозиум INFO-89, т.1, ч.1. — Минск, 1989. — С.572-577.

[Лазарев88] Лазарев А. Эти доверчивые компьютеры... // Эхо планеты. - 1988. - N 34. — С.44-46.

[Ландсберг90а] Ландсберг Г.Л. Компьютерные вирусы и методы борьбы с ними. — Протвино: ИФВЭ, 1990. — 44 с.

[Ландсберг90б] Ландсберг Г.Л. Универсальная антивирусная программа PHENIX. — Протвино: ИФВЭ, 1990. — 26 с.

[Лесков91] Лесков С. Сети для "черного мстителя" // Известия. - 1991. - 2 февраля.

[Лигская89] Лигская А.В., Миримская О.М. Компьютерный вирус // США — экономика, политика, идеология. - 1989. - N 11. — С.69-77.

[Лилитко89] Лилитко Е.П. "Бой в памяти" — игра созидательная // Мир ПК. - 1989. - N 3. — С.131-132.

[Лозинский90] Лозинский Д. Одна из советских антивирусных программ: AIDSTEST // КомпьютерПресс. - 1990. - N 6. — С.17-20.

[МиК90] На срок до пяти лет... // Мы и компьютер. - 1990. - N 1. — С.28.

[Недков89а] Недков С.Н. Програми за проникване в изчислителните системи // АИТиАС. - 1989. - г.5. - N 3. — С.38-43.

[Недков89б] Недков С.Н. Модели на разпространението на вируси в изчислителни системи // АИТиАС. - 1989. - г.5. - N 7. — С.18-23.

[Недков89в] Недков С.Н. Компютърна хигиена: вируси // Компютър за вас. - 1989. - г.5. - N 56. — С.13-16.

[Недков89г] Недков С.Н. Антивирусни програми // Компютър за вас. - 1989. - г.5. - N 910. — С.6-10.

[Недков89д] Недков С.Н. Средства защиты персональных компьютеров от вирусов // Международный симпозиум INFO-89, т.1, ч.1. — Минск, 1989. — С.566571.

[Недков90а] Недков С.Н. Вирусът за $ 96 000 000 по мрежата Arpanet/Internet // Компютър за вас. - 1990. - г.6. - N 3-4. — С.5-8.

[Недков90б] Недков С.Н. На вирусния фронт нещо ново // Компютър за вас. - 1990. - г.6. - N 5-6. — С.2-4.

[Нельсон90] Нельсон Т. Диагностика вирусов // Мир ПК. - 1990. - N 1. — С.60-62.

[Николаев90] Николаев А. Осторожно — вирус ! // КомпьютерПресс. - 1990. - N 6. — С.3-16.

[Осипенко90] Осипенко А.С. Компьютерные вирусы // Мир ПК. - 1990. - N 3. — С.23-30.

[Охрименко89] Охрименко С.А. Защита персональных ЭВМ от программных злоупотреблений (компьютерных вирусов). — Кишинев: МолдНИИТЭИ, 1989. — 27 с.

[Павлов89] Павлов А. Компьютерная чума в СССР // Химия и жизнь. - 1989. - N 7. — С.20-21.

[Селль90] Селль М. Антивирусные программы // Компьютер. - 1990. - N 2. — С.48-50.

[Скенлон] Скенлон Л. Персональный ЭВМ IBM PC и XT. Программирование на языке ассемблера / пер. с англ. — М.: Радио и связь, 1989. — 336 с.

[Стефанков90] Стефанков Д. Пятница, 13е // Интерфейс. - 1990. - N 1. — С.38-42.

[Стоянов90] Стоянов А. За лудия и вирусните зелници // Компютър за вас. - 1990. - г.6. - N 1-2. — С.6-7.

[Сяо82] Сяо Д., Керр Д., Мэдник С. Защита ЭВМ / Пер. с англ. — М.: Мир, 1982. — 263 с.

[Томов90] Томов А. Ваксината Hunter // Компютър за вас. - 1990. - г.6. - N 5-6. — С.6-11.

[Уолкер80] Уолкер Б.Дж., Блейк Я.Ф. Безопасность ЭВМ и организация их защиты / Пер. с англ. — М.: Связь, 1980. — 112 с.

[Фигурнов90] Фигурнов В.Э. IBM PC для пользователя. — М.: Финансы и статистика, 1990. — 240 с.

[Фигурнов90а] Фигурнов В.Э. Работа пользователя с IBM PC: Комплект документации и программ. — М.: СП "Интерквадро", 1990. — 620 с.

[Хоффман80] Хоффман Л.Дж. Современные методы защиты информации / Пер. с англ. — М.: Сов.радио, 1980. — 264 с.

[Цал90] Цал М.И. Вирусная атака // НОВИНТЕХ. - 1990. - N 1. — С.35-37.

[Чижов88] Чижов А.А. Некоторые соображения по поводу компьютерных вирусов // В мире персональных компьютеров. - 1988. - N 1. — С.121-124.

[ЧижовМ90] Чижов М.В. Защита от компьютерных вирусов.- Дубна: ОИЯИ, 1990.- 4 с.

[ЧиК90] Компьютерный терроризм // Человек и компьютер. - 1990. - N 40. — С.24.

[Шерстюк90] Шерстюк Ф.Н. Вирусы и антивирусы на IBM-совместимых ПК // Интеркомпьютер. - 1990. - N 2. — С.46-47.

[ЭиЖ90] Компьютерный шпионаж // Экономика и жизнь. - 1990. - N 40. — С.24.

[Эхо90] Компьютерный вирус милитаризуется // Эхо планеты. - 1990. - N 23. — С.45.

ПРИЛОЖЕНИЕ

НЕКОТОРЫЕ ОТЕЧЕСТВЕННЫЕ АНТИВИРУСНЫЕ СРЕДСТВА, РАСПРОСТРАНЯВШИЕСЯ ЧЕРЕЗ ЭЛЕКТРОННЫЙ БЮЛЛЕТЕНЬ СОФТПАНОРАМА

ДЕТЕКТОРЫ

LD — пакетный полидетектор с возможностью эвристического определения новых типов вирусов. Разработчик: Сусликов Евгений Николаевич (Кемерово). Способ распространения: FREEWARE — СП; автор, тел.(3842)23-44-03 (сл).

DL — полидетектор с вводом сигнатур для контекстного поиска, диалоговым интерфейсом и возможностью просмотра дампа программы, в которой найдена сигнатура на экране. Разработчик: Шеховцов Александр Людвигович (Киев). Способ распространения: FREEWARE — СП; тел. автора (044)266-00-97(сл).

ФАГИ

V — пакетный полифаг с диалоговым интерфейсом. Разработчик: Касперский Евгений Валентинович (Москва). Способ распространения: COMMERCIAL — МГП "Алиса", тел.(095)248-32-52.

AIDSTEST — пакетный полифаг. Разработчик: Лозинский Дмитрий Николаевич (Москва). Способ распространения: COMMERCIAL — Научный центр СП "Диалог" при ВЦ АН СССР, тел.(095)137-01-50.

ANTI-KOT — пакетный полифаг с диалоговым интерфейсом. Разработчик: Котик Олег Генрихович (Москва). Способ распространения: COMMERCIAL. Распространители: СП "Интермикро", тел.(095)267-32-10; НТЭЦ "Сэканс", тел.(095)183-10-89.

AV — пакетный полифаг. Разработчик: Сысоев Игорь Викторович (Москва). Способ распространения: FREEWARE.

AVB — универсальный бутовый детектор-фаг. Разработчик: Свиридов Игорь Анатольевич (Киев). Способ распространения: SHAREWARE — СП; тел. автора: (044)263-87-70.

SOS — полифаг с диалоговым интерфейсом и возможностью автонастройки на детектирование новых обнаруженных вирусов. Разработчик: Сусликов Евгений Николаевич (Кемерово). Способ распространения: FREEWARE — СП; тел.автора: (3842)23-44-03.

NEATFAG — модульный пакетный полифаг. Разработчик Пономаренко Виталий Витальевич, Киев. Способ распространения: FREEWARE — СП, тел.автора: (044)484-19-84.

РЕВИЗОРЫ

CHECK — пакетный ревизор. Разработчик: Гонтарь Борис Борисович (Киев). Способ распространения: Public Domain — СП; тел.автора, (044)265-68-73(сл).

DLI — пакетный ревизор. Разработчик: Герасимов Вадим Викторович, Москва.

J-CHECK — ревизор. Разработчик: Базалий Юрий Алексеевич, Киев,тел.(044)227-25-41 FREE-SRC.

SPEEDCHK — ревизор с возможностью ускоренной проверки файлов. Разработчик: Шнайдер Лев Семенович, Киев, тел.(044)274-91-87 FREE-SRC.

СТОРОЖА

CHECK21 — сторож 21 прерывания. Разработчик: Двоеглазов Игорь Михайлович, Киев, тел.(044)517-02-05 Способ распространения: FREEWARE

-D,-D3. — резидентный сторож. Разработчик: Касперский Евгений Валентинович, Москва. Способ распространения: COMMERCIAL — МГП "Алиса", тел.(095)248-32-52.

IWP — резидентный сторож с расширенными возможностями защиты. Может использоваться совместно со специальной платой PORT WATCH CARD. Разработчик: Водяник Аркадий Григорьевич, Мариуполь. Способ распространения: FREEWARE (без платы), COMMERCIAL (с платой PORT WATCH CARD) — НПК БИС (Донецк), тел.(0622)93-10-21.

SBM — сторож 21 прерывания. Разработчики: Еременко Василий Евгеньевич, Мостовой Борис Михайлович, Киев, тел.(044)416-13-69. FREEWARE.

ВАКЦИНЫ

NEATVAC — резидентная поливакцина. Разработчик Пономаренко Виталий Витальевич, Киев, тел.(044)484-19-84. FREEWARE

VITAMINB — вакцина против бутовых вирусов, основанная на замене бутсектора на специальный. Разработчик: Сесса Александр В., Днепропетровск. FREEWARE.

UNIVAC — универсальная вакцина для файловых вирусов, дописывающихся в конец файла. Разработчик: Бабанин Валерий Михайлович, Тверь, тел.(222)6-61-64. FREEWARE.

ПРОЧИЕ АНТИВИРУСНЫЕ ПРОГРАММЫ

COM4VIR, EXE4VIR, SYS4VIR

Ловушки для вирусов. Разработчик: Волынский Владимир Викторович, Москва, тел.(095)219-99-62. FREEWARE

VI — вирусный интегратор. Разработчик: Шеховцов Александр Людвигович, Киев. тел.(044)266-00-97(сл). FREEWARE

ПРИМЕЧАНИЯ

1. Программы разбиты по типам, а внутри каждого типа упорядочены по алфавиту. Некоторые программы разных авторов имеют одинаковые имена. В таких случаях программы упорядочивались по фамилии разработчика.

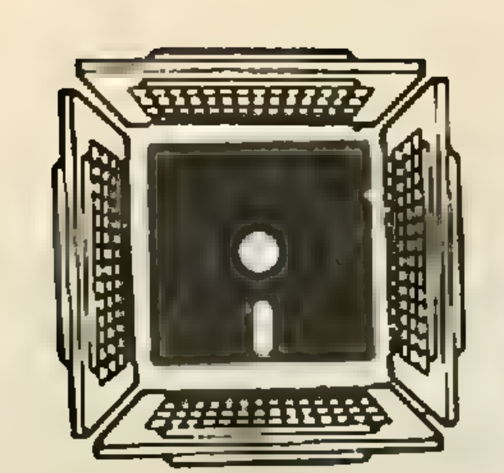
2. При указании способа распространения используются следующие обозначения:
COMMERCIAL — коммерческий продукт;
FREEWARE — свободно;
FREE SOURCE — свободно с исходными текстами;
SHAREWARE — с частичным субсидированием разработки пользователями.

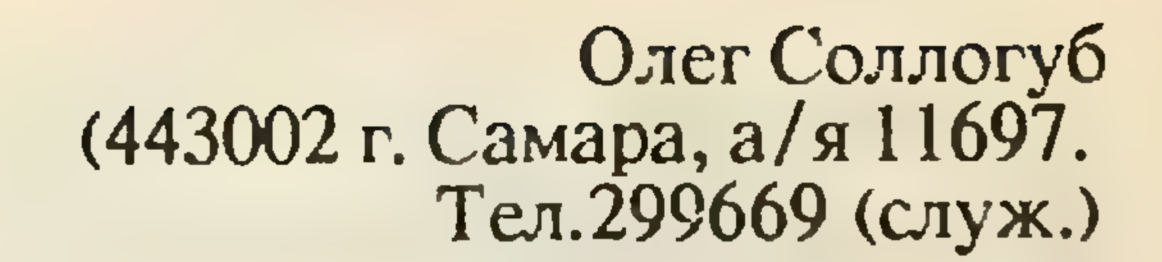
3. После указания способа распространения через тире указаны распространители. Если распространителей несколько, то они отделяются друг от друга точкой с запятой. Указание в качестве распространителя СП означает, что версии данного программного продукта публиковались в электронном бюллетене СОФТПАНОРАМА. Для некоммерческих продуктов более поздние версии обычно можно получить у автора.

4. По вопросам подписки на бюллетень Софтпанорама и приобретения отдельных выпусков следует обращаться к официальным распространителям бюллетеня:

— Авиацентр НТТМ: 252680, Киев-58, ГСП, просп. космонавта Комарова, 1, КИИГА, корп.3, ком.104, тел.(044)484-94-46, Белоусов Анатолий Федорович, тел.(044)484-90-98, Ткаченко Галина Эросовна.

— Научный центр СП "Диалог" при ВЦ АН СССР: 117967, Москва, ГСП-1, ул. Вавилова, 40, комн.103а, тел.(095)137-01-50.





Олег Соллогуб
(443002 г. Самара, а/я 11697.
Тел.299669 (служ.)

КАК ОБМАНУТЬ НЕПОСЛУШНУЮ РУССКУЮ "Р"

Пользователи IBM PC-совместных ПЭВМ часто сталкиваются с тем, что многие западные программные продукты не воспринимают строчную русскую букву "р" при вводе с клавиатуры. Примером может служить, например, известная система The Norton Commander. Для преодоления этой проблемы вряд ли целесообразно заниматься адаптацией всех используемых программ — это трудоемкая задача даже для опытного программиста. Однако есть очень простой выход из положения, который состоит в замене русской "р" латинской буквой "р". В большинстве случаев такая замена вполне допустима, поскольку эти буквы, хотя и имеют разные коды, обычно выглядят идентично как на экране дисплея, так и при выводе на принтер.

Однако переходить всякий раз для ввода буквы "р" из кириллицы в латиницу и обратно, конечно, очень утомительно. Поэтому лучше всего внести соответствующее исправление в драйвер клавиатуры, который установлен на вашем компьютере. Это можно сделать, например, с помощью утилиты PCTools. Рассматривая коды программы, вы, скорее всего, обнаружите таблицу перекодировки, в которой будет присутствовать строка символов "вуапршол" (коды A2 E3 A0 AF E0 E8 AE AB — "альтернативной" кодировкой). В этой строке код E0 надо заменить на 70. После перезагрузки ПЭВМ вместо русской "р" с клавиатуры будет вводиться латинская "р".

Если вам почему-то не удалось разобраться в драйвере клавиатуры, проблема может быть разрешена иначе, путем создания небольшой специальной программы. Для этого воспользуйтесь отладчиком DEBUG, входящим в состав операционной системы VS DOS. Вызвав DEBUG и дождавшись приглашения, которое имеет вид дефиса (черточки), аккуратно наберите приведенный ниже текст, не забывая нажимать клавишу ввода в конце каждой строки. Набор производится латинскими буквами (прописными или строчными — безразлично), количество пробелов между командами и параметрами значения не имеет. Строка, обозначенная <Enter> — пустая, надо лишь нажать клавишу ввода. Если в процессе работы вдруг появится сообщение "Error", нужно нажать ввод, ввести команду G (выход из DEBUG) и повторить все еще раз, стараясь не допускать ошибок.

Когда вы закончите ввод текста, произойдет выход в DOS, а в текущем каталоге появится файл с именем P-OK.COM — это и есть ваша программа-перекодировщик. При запуске ее никаких сообщений не выдается, но программа остается резидентно в памяти ПЭВМ и подменяет русскую "р" при обращениях к клавиатуре. Если окажется, что запуск программы вызывает зависание системы, это значит, что в процессе ввода допущена какая-то ошибка, и нужно все повторить с самого начала.

Обратите внимание, что программа P-OK.COM должна загружаться после всех других драйверов клавиатуры, если они имеются. Программа занимает в оперативной памяти всего лишь 224 байта, и ее можно загружать всякий раз при запуске ПЭВМ с помощью файла AUTOEXEC.BAT.

Текст программы

(последовательность команд отладчика DEBUG):

```
A
MOV AX,3516
INT 21
MOV [11D], BX
MOV [11F], ES
MOV DX,121
MOV AX,2516
INT 21
MOV DX, 14
MOV AX,3100
INT 21
DW O,O
OR AH,AH
JNZ 132
PUSHF
CS:CALL FAR [11D]
CMP AL,EO
JNZ 131
MOV AL,70
IRET
CS:JMP FAR [11D]
<ENTER>
 RCX
37
N P-OK.COM
W
Q
```





В восьмом номере "Вычислительной техники" за 1990 г. я поделился информацией о пульте управления ПУ-1 (джойстик) и координатном устройстве ввода УВК-1 ("мышь") для БК-0010. Хочу предложить вашему вниманию описание других периферийных устройств, доступных сегодня пользователям БК.

Д.Ю.Усенков

О некоторых периферийных устройствах для БК-0010

1) Не так давно в магазине "Электроника" появился в продаже новый джостик. Он немного меньше, чем описанный в N 8 джойстик ПУ-1, и оснащен такой же анатомической рукояткой. Кнопок у него не четыре, как у ПУ-1, а только три (одна на рукоятке сверху и две на корпусе), но эти три кнопки, в отличие от ПУ-1, уже распараллелены, то есть выведены на отдельные провода. Шнур этого нового джойстика представляет собой плоский кабель без какого-либо разъема на свободном конце. Предполагается, что пользователь сам распаяет кабель по требуемым для его компьютера контактам. При распайке можно воспользоваться нижеприведенной таблицей, где указаны контакты для подключения джойстика к порту БК-0010.

Обозначение контакта джойстика	Вводимая команда	Контакт порта БК-0010
↑	вперед	B23
←	влево	B24
↓	назад	B17
→	вправо	A24
•←	левая кнопка	B22
⊥	общий	A18,A19,B18 или B19
→•	правая кнопка	B20
↑	верхняя кнопка	A20

Эта таблица приводится в магазине. В пояснении к таблице сказано, что это — стандартная распайка. Однако пока не все игры соответствуют этому стандарту, поэтому для них, возможно, потребуется изменение в программе игры. Некоторые игры (XONIX и ZOOM, в частности) позволяют использовать джойстик с любой распайкой, "подлаживаясь" под нее. При запуске игры ZOOM, которая, кстати, идеальная для работы с джойстиком, для предложенной распайки джойстика нужно выполнить следующую последовательность действий:

- выйти в режим "Управление" (с помощью клавиш ↑, ↓ и <ввод>);
- с помощью тех же клавиш вызвать из меню режим "нестандартный джойстик";
- в ответ на запросы ЭВМ ввести: "Состояние порта вывода" равно 0, "Маска ввода" равна 177700;

- аккуратно "покачивая" рукоятку и нажимая кнопку, указать машине какими действиями джойстика вы будете задавать команды из предложенного компьютером списка;

- в ответ на запрос "Выбор управления" указать "от джойстика" или "параллельное" (то есть и с джойстика и с клавиатуры).

После этого можно начинать игру. (Примечание: окончание игры, переходы от одного меню к другому и выход из меню производится выбором нужной команды; если команда "выход" в меню не указана, значит выход из меню производится автоматически при окончании отработки выбранной команды.)

Стоит новый джойстик несколько дороже ПУ-1: его цена 64 рубля. Повышение стоимости вызвано, по-видимому, применением в нем контактов на герконах, значительно более надежных в работе, чем примененные в ПУ-1 обычные "пластинчатые" контакты.

2) ПРИНТЕРЫ. В магазине-салоне "Электроника" представлены для продажи несколько различных видов принтеров (печатающих устройств). Большинство из них, к сожалению, для рядового пользователя БК практически недоступны из-за своей высокой цены. Только два из них можно считать "сравнительно дешевыми":

1. Принтер, названный в техническом паспорте и руководстве пользователя "Устройством вывода информации печатающим "Электроника МС-6312", представляет собой небольшую коробочку с габаритами 53,5x170x277 мм удобно размещаемую на столе рядом с компьютером. Масса его — не более трех килограмм. Принтер МС-6312 так называемого термоструйного типа: печать отдельной точки на бумаге прозводится "выстреливанием" разогретого специального состава (типа чернил). Этот принтер позволяет печатать как алфавитно-цифровую, так и графическую информацию на обычной бумаге формата А4, применяемой для печати на обычных пишущих машинках, или на бумаге в виде рулона такой же ширины.

Технические данные:

Число символов в строке: 80;
Скорость печати: 150 знаков в секунду для шрифта типа ELITE;
Набор печатаемых знаков: не менее 162;
Шаг печати (расстояние между символами): 2,12 мм;
Шаг между строками: 4,23 мм;
Матрица символа: 16x12 точек;
Минимальная толщина линий: 0,4 мм;
Варианты печатаемого шрифта:
1 — уплотненный (обычный вариант);
2 — расширенный;
3 — подчеркнутый;
4 — "жирный" (с двойным пропечатыванием каждой точки);
5 — линия подчеркивания;
6 — верхние индексы;
7 — субскрипты.
Цена: 1500 рублей.

Печать производится путем передачи с ЭВМ в принтер по соединяющей их линии кода символа в стандарте ASCII. Подача различных управляющих сигналов производится с помощью так называемых ESCAPE — последовательностей широко применяемых, например, в операционной системе MS-DOS (подробнее об этой операционной системе и о ESCAPE-последовательностях вы можете прочитать в книге: Брябрин В.М. "Программное обеспечение персональных ЭВМ", Москва, "Наука", 1989 г.) То, что в БК не реализована система ESCAPE-последовательностей, неудобство сравнительно небольшое: есть кооперативы, которые производят адаптацию такого принтера к БК-0010. Координаты кооперативов можно узнать в том же магазине "Электроника". Значительно большим недостатком такого принтера является то, что сам пишущий узел-"чернильница" одноразовый и по мере израсходования его, подобно стержню шариковой ручки, приходится заменять. Стоимость нового пишущего узла 25 рублей, он продается в той же "Электронике".

2. Второй тип принтера — МС-6313 — устройство более дорогое — 1765 рублей, зато без "одноразовых" деталей. Это так называемый матричный принтер, где изображение символа получается воздействием на бумагу сквозь пишущую ленту ряда специальных, управляемых электромагнитами игл. Принтер МС-6313 значительно больше по размерам и массе, чем МС-6312. Его габариты 400х460х100 мм и масса около 8 кг. Игл в пакете девять, и они "рисуют" символ, печатая его ряд за рядом. Бумага для него используется, как и для МС-6312, простая листовая формата А4 или рулонная. Лента красящая-одноцветная, такая же, как на обычных пишущих машинках, только с более прочной тканевой основой (для предотвращения разлохмачивания краев). Ее установка на принтер производится не так, как на пишущих машинках: без бобин, с жесткой фиксацией обоих концов ленты на корпусе. О последовательности выполнения этой операции рассказано достаточно подробно в прилагаемом к принтеру руководстве. Печатать можно как алфавитно-цифровые, так и графические символы. По своим характеристикам данный принтер близок к МС-6312. Отличие — в способе переключения типа шрифта. Здесь оно производится вручную путем переключения расположенных под крышкой переключателей. Для печати символа (алфавитно-цифрового или полуграфики) в принтер передается его код ASCII. Канал передачи-типа IRPC-M (подобный применяемому в составе КУВТ-86 БК-0010 для связи с ДВК) или со стыком С2, причем необходимые для соединения кабели с разъемами прилагаются к принтеру. Кроме того, можно печатать и непосредственно твердую копию экрана. Вместо кода символа для этого передается число, кодирующее участок изображения, соответствующий гребенке игл, при этом иглы, соответствующие единичным битам этого числа, производят печать точек на бумаге, тогда как иглы, соответствующие нулевым битам, точки не печатают. Чтобы произвести копирование экрана, нужна программа, подобная опубликованной в "Вычислительной технике" № 5 за 1990 год программе TUCOPY1 (см. стр. 32).

В отличие от принтера МС-6312 этот принтер легче подключить к БК-0010. Раскладка контактов разъема этого принтера несколько отличается от приведенной в N 5 за 1990 г. для УВВПЧ 30-004. Привожу эту раскладку в виде таблицы:

Контакт принтера	Обозначение	Активный уровень	Назначение
3	D1	высокий	шина данных
5	D2	высокий	
7	D3	высокий	
9	D4	высокий	
11	D5	высокий	
13	D6	высокий	
15	D7	высокий	
17	D8	высокий	
23	STROBE	низкий	строб
27	INIT	низкий	сброс
29	SLCTIN	низкий	выбор
30	AUTO	низкий	автоперевод строки
19	ERROR	низкий	ошибка
21	BUSY	высокий	"занят"
25	ACRNLG	низкий	подтверждение
2	CH.GND	—	экран

3) **Графопостроитель.** Он предназначен специально для БК-0010.01. Графопостроитель представляет собой компактное устройство размером 80х180х400 мм и массой 2,8 кг, которое можно удобно разместить на столе. Он позволяет выводить на листы обычной бумаги размером 210х297 мм (формат А4 по ГОСТ 2.301-68) графические

изображения (линии, окружности, эллипсы и т.п.), тексты путем вычерчивания каждой буквы, графики функций путем вычерчивания их отрезками прямых и т.д. При этом текст можно располагать не только "по горизонтали" (вдоль листа), но и "по вертикали". Рабочее поле записи (лист используется не весь, остаются небольшие поля по краям) — 185x260 мм. Принцип работы этого графопостроителя — роллинговый: по одной из координат перемещается сам лист бумаги путем его перематывания вперед-назад между прижимными роликами, а по второй по специальной направляющей перемещается зажим для пишущего узла — фломастера, шариковой ручки, наполненного тушью рапидографа (улучшенный аналог обычного рейсфедера), или даже обычного карандаша. По способу работы он напоминает станок с ЧПУ: по командам перемещения по координатам X и Н шаговые двигатели отрабатывают требуемое число микроперемещений-шагов по 0,1 мм (точность довольно высокая: порядка сотых долей миллиметра). Команда типа "поднять-опустить" перо позволяет чертить линию на бумаге или переносить перо от одной точки к другой без вычерчивания. Скорость черчения — до 100 мм в секунду. Конечно, по сравнению с "большими" графопостроителями такая скорость "не впечатляет", но для бытового устройства достаточно высока. Так как графопостроитель сделан специально для БК-0010.01, никаких проблем с его подключением или адаптацией нет. Подключается он непосредственно к разъему внешнего порта БК. Проблем с управляющими его работой программами тоже нет: в комплект к нему входит магнитофонная кассета с записями программы-драйвера в кодах и программы-рекламы, являющейся примером использования этого драйвера. Драйвер рассчитан на применение его в виде USR-функции в Бейсик-Вильнюсе БК-0010.01 и позволяет выводить на графопостроитель окружности (эллипсы), линии, точки и задаваемый текст. Все данные передаются драйверу через специально отведенные ячейки ОЗУ с помощью операторов POKE, а текст задается непосредственно в виде аргумента функции USR. Этот же драйвер, если его немного доработать (упростить способ его вызова, который для подпрограмм типа USR Бейсик-Вильнюса более сложен, чем для подпрограмм, используемых в программах на Ассемблере), может быть применен и для программ в кодах, на КОФОКе, XFOKALе и других языках. Стоимость графопостроителя — 1000 рублей.

4) Видеомонитор. Из-за отсутствия в отечественных телевизорах видеовхода для подключения БК пользователю обычно приходится "лезть" с паяльником в схему. Это достаточно неудобно, сложно (особенно для цветного телевизора) и дает изображение не очень высокого качества. Купить же где-либо блок-адаптер для побключения БК на антенный вход (как это сделано, например, для "Микроши") тоже невозможно: завод, выпускающий БК, давно уже обещал их выпускать, но дальше появления на прилавке "Электроники" опытного образца дело пока не пошло. Кроме того, использовать для БК обычный телевизор не очень-то удобно: на него, кроме вас, "имеют виды" и другие члены семьи. Более удобно и надежно использовать для БК-0010 видеомонитор (специально рассчитанный на работу с компьютером телевизор без высокочастотных усилителей и переключателя каналов, имеющихся в обычном телевизоре, зато обеспечивающий более высокое качество изображения). В магазине "Электроника" представлено несколько типов видеомониторов, Но только один из них имеет цветное изображение. Видеомонитор "Электроника 32 ВТЦ-201" (МС6113). Это переносной аппарат на базе телевизора "Юность", специально предназначенный для подключения БК, "Агата" и других подобных им компьютеров. На задней стенке монитора имеется два разъема: для БК и для "Агата". Монитор оснащен цветным кинескопом с самосведением лучей, электростатическим принципом создания цветного изображения и импульсным блоком питания. Размер экрана — 154±8 x 219±10 мм, число выводимых точек — 256x256 или 32 символа x 32 строки (у БК соответственно, часть поля остается незаполненной). Количество цветов — не менее 8 (для "Агата"), а для БК-0010.01 — три, но программным способом можно получить и больше. Вход сигнала для БК-низкочастотный, RSB (по трем отдельным линиям) и "синхронизация". На передней стенке находятся выключатель и индикатор питания (светодиодный), регуляторы яркости и контраста, закрытое заглушкой гнездо для наушников и место для установки динамика. На задней стенке предусмотрены регуляторы цветности ("зеленый-пурпурный" и "красный-синий"), разъемы для подключения БК и "Агата", блок предохранителей, два гнезда для регулировки положения изображения на экране (вес монитора около 13 кг). Что касается его стоимости, трудно сказать что-либо определенно: это

экспериментальная модель, и ее стоимость может меняться как в "ту", так и в "другую" сторону. Пока что его стоимость — порядка 700 рублей.

5) Для тех, кто хочет сам собрать компьютер или какое-либо устройство для него, в "Электронике" есть возможность приобрести пластмассовый корпус, блок клавиатуры, шаговые двигатели и даже комплект для изготовления и подключения к компьютеру модема (модем — устройство, похожее на телефон; позволяет передавать программы, файлы с текстами и прочую информацию от компьютера к компьютеру по телефонной линии). Для тех же, кто работает на компьютерах, оснащенных дисководами и кому приходится носить с собой гибкие диски в "Электронике" бывает в продаже полезная мелочь-пластмассовая коробочка для хранения и переноски дискет. Стоит она 4 рубля 50 копеек. Имеется в "Электронике" и большой набор программ (правда, в основном не для БК, а для машин типа "Спектрум"). Для БК есть только два комплекта: графический редактор и комплект программ для создания картинок-заставок к программам, меню и прочих текстовых документов. Стоят они порядка 90-200 рублей за комплект.

Адрес магазина-салона фирмы "Электроника":

Москва, Ленинский проспект, 87, тел. 134-60-11 (бытовые компьютеры и периферийные устройства). Проезд: метро до станций "Университет", "Проспект Вернадского" и "Юго-Западная" далее на автобусах и троллейбусах.

ВЫСОКОЕ КАЧЕСТВО!

Львовский НПК "Монитор" предлагает профессиональную автоматизированную стстему проектирования РЭА.

Состав аппаратных средств:

- эмулятор однокристалльных микро-ЭВМ серии К1816ВЕ48;
- эмулятор однокристалльных микро-ЭВМ серии К1816ВЕ51
  - *работают под управлением ПЭВМ типа IBM PC AT/XT.*
- универсальные программаторы:
  модель А для программирования ППЗУ и ОЭВМ: К573РФ2, РФ5, РФ3, РФ4, РФ6, РФ8, К556РТ4-РТ7, РТ11-РТ18, К155РЕ3, i2764, КР1816ВЕ48
  - *работает под управлением ПЭВМ типа IBM PC AT/XT и автономно под управлением собсвенной микро-ОЭВМ.*
  модель В для программирования ППЗУ и ОЭВМ: К573РФ2, РФ5, РФ4, РФ6, РФ8, i2716, 2732, 2764, 27128, 27256, 27512, К155РЕ3, К556РТ4, К556РТ5, РТ11-РТ18, К1816ВЕ48, К1816ВЕ51, К1813ВЕ1, i8748, i8751, i2920
  - *работает только под управлением ПЭВМ типа IBM PC AT/XT.*

Состав интегрированных программных средств, работающих в среде MS DOS:
- пакеты программ поддержки функционирования аппаратных эмуляторов микро-ОЭВМ;
- пакеты программ поддержки функционирования универсальных программаторов ППЗУ и ОЭВМ;
- пакеты программных кросс-средств для ОЭВМ К1816ВЕ48, К1816ВЕ51.
  - *классический набор, дружественный интерфейс, комфортное меню.*

Конфигурацию САПР выбирает заказчик.
Имеются системные и игровые программы для ПК-01 "Львов".
Наш опыт и репутация - гарантия ваших успехов!
Обращаться по адресу: 290044, Львов, а/я 8863, НПК "Монитор".
Телефоны: 35-35-79 с 9 до 17 часов;
34-29-42 с 19 до 8 часов.

В.В.Сапогов

HELP — драйвер для БК-0010

Каждый, кто когда-либо сталкивался с работой на IBM — совместимых компьютерах наверняка оценил преимущества используемых там так называемых HELP-подсказок. Стоит вкратце напомнить что представляют из себя HELP-подсказки. При нажатии на определенную клавишу (обычно F1) на экране появляется окно, в которое выводится текст, разъясняющий работу активной в данный момент программы, подсказывающий дальнейшие действия и т.д. Текст в этом HELP-окне можно листать, используя функциональные клавиши компьютера. После нажатия на вторую определенную клавишу (обычно Esc) HELP-окно исчезает с экрана, при этом в исходном виде восстанавливается вся та экранная область, которая была закрыта HELP-окном, после чего активная программа продолжает свою работу.

Подобным же образом можно организовать работу БК, несмотря на очень скромные возможности этого компьютера. Для этого и предназначен HELP-драйвер.

Предлагаемая программа содержит полный текст HELP-драйвера, а также демонстирует его работу.

Общий объем памяти, занимаемый HELP драйвером составляет 386 байт, кроме того для его работы необходим буферный участок памяти, в котором сохраняется содержимое области экрана, закрываемое HELP-окном. Объем этого буферного участка должен быть 1312 байта. Такой значительный объем буферной памяти объясняется тем, что в ОЗУ БК не сохранятся информация о выводимых на экран символах, поэтому приходится сохранять область экрана как графическую "картинку". Драйвер позволяет выводить текст в окно размером 4*32, располагающееся в центре экрана, этот текст может содержать больше 4-х строк, "прокрутка" текста в окне выполняется с помощью клавиш управления курсором ↓↑. Тексты, выводимые в HELP-окно длжны быть соответствующе подготовлены и помещены в ОЗУ с определенного адреса.

Для вызова HELP-экрана и его отмены используется одна и та же клавиша КТ. При первом нажатии на нее HELP-окно появляется на экране, при повторном нажатии — исчезает при этом полностью восстанавливается содержимое экрана до вызова HELP-окна. Текст в HELP-окно выводится с помощью темных букв на светлом фоне. После отмены HELP-окна драйвер оставляет неизменными действовавшие до его вызова режимы дисплея, а также положение курсора. Драйвер полностью перемещаем, т.е. загружать его в память можно с любого адреса.

Для разъяснения конкретных деталей использования HELP-драйвера рассмотрим текст программы. Операторы DATA 30-420 содержат коды самого драйвера. В операторах 430-470 выполняется здагрузка драйвера в ОЗУ и назначение стартового адреса. Операторы DATA 480-550 содержат тексты, выводимые в два HELP-окна. Строки, содержащиеся в операторах DATA 480-510 — выводятся в первое окно, в операторах 520-550 — во второе. Так как в строковые константы, содержащиеся в операторах DATA нельзя ввести с клавиатуры некоторые символы, например "перевод строки" (код 10), три символа выбраны в качестве служебных. ♥ (код 169, клав.АР2 I) — перевод строки; ♣ (код 180, клав.АР2 Т) — переход к следующему HELP-экрану, т.е. в одно HELP-окно выводится текст, заканчивающийся символом ♣; ♦ (код 184, клав.АР2 Х) — конец HELP-текста, этот символ должен стоять самым последним в HELP-тексте.

Тексты, выводимые в HELP-окно должны быть размещены с конкретного адреса ОЗУ. Адрес для первого HELP-экрана назначается в операторе 570, а само размещение выполняет подпрограмма, начинающаяся с оператора 2000. Эта подпрограмма получилась довольно громоздкой из-за того, что оператор POKE не позволяет адресоваться к нечетным адресам памяти. Операторы 590, 600 — выполняют установку HELP-драйвера и передачу ему адреса начала HELP-текста. Подпрограмма, начинающаяся с адреса 2200 заполняет весь экран символом, код которого присваивает-

ся переменной 11%. Это необходимо, чтобы проконтролировать правильность восстановления экрана после отмены HELP-окна. Операторы 630-650 контролируют код нажатой клавиши, дальнейшее выполнение программы возможно только после нажатия клавиши ВВОД. В этом месте программы с нажатием КТ можно вызвать HELP-экран и просмотреть весь HELP-Текст, используя клавиши ↑ ↓. Операторы 660-750 выполняют те же действия, что и операторы 560-650, но для второго HELP-окна. В операторах 760-800 выполняется запрос на выгрузку HELP-драйвера. Драйвер выгружается, если в качестве аргумента ему передается нуль, что делается в операторах 810, 820. Если выход из программы выполняется без выгрузки драйвера, то он остается загруженным и после ее завершения, т.е. в режиме ввода команд Бейсика нажатие на клавишу КТ также будет вызывать появление HELP-окна. При нажатии на все остальные клавиши драйвер никак себя не проявляет. Выгрузить драйвер можно запустив программу с оператора 810 или непосредственно набрав операторы 810, 820 в режиме ввода команд. После выполнения программы можно сохранить драйвер на магнитной ленте командой BSAUE "HELPDR", &O32000, &O32600.

Необходимо отметить, что приведенная программа предназначена для работы в режиме "64 символа в строке", т.е. перед началом ее работы необходимо нажать клавиши АР2. Так как на работу драйвера не влияют режимы работы дисплея, то он может работать и в режиме "32 символа в строке", при этом естественно размеры HELP-окна уменьшатся до 4*16, в остальном работа драйвера останется без изменений.

При необходимости можно изменить назначение клавиш, управляющих работой драйвера. Клавиша, код которой подчеркнут в операторе 70 вызывает появление HELP-окна, клавиша, код которой подчеркнут в операторе 390 вызывает отмену HELP-окна. Изменяя указанные коды можно выбирать по своему усмотению клавиши, управляющие драйвером. Число, выделенное в операторе 160 определяет адрес начала буферной области, в программе этот адрес выбран равным &O33000=13824.

В заключение необходимо отметить, что при применении описанного драйвера в прикладных программах следует по-возможности располагать сам драйвер и тексты к нему в старших адресах памяти — ближе к &O40000, чтобы не перекрыть текст самой программы. Однако начальные адреса для их хранения следует выбирать осторожно, потому что как показала практика работы с драйвером, некоторая часть старших адресов используется Бейсиком для служебных целей и если изменить содержимое этих адресов, то можно частично или полностью потерять текст программы.

```
1Ø CLEAR 1ØØØ
2Ø DIM A$(256%)
3Ø  DATA   4544, 26Ø48,     24,  3Ø21,    772
4Ø  DATA   4944,  4127,    176,   135,   2591
5Ø  DATA    176,   135
6Ø  DATA                     Ø,     Ø,   9664
7Ø  DATA      3,   769,    135,  4548,  -6716
8Ø  DATA     14,-3Ø714,   558Ø,     1,   6118
9Ø  DATA    176,  2591,    176,-3Ø698,   4198
1ØØ DATA   4262,-3Ø692,   4134,  6Ø81,    -76
11Ø DATA  17857,  -256,   9665,   216,   18ØØ
12Ø DATA   5568, 18944,   3ØØ9,   778,  26Ø48
13Ø DATA     64, 32323,    262,  5568,  16384
14Ø DATA  -6719,   216,    769,   5Ø2,  26Ø48
15Ø DATA   6736,  9664,-32768,-32764,  17856
16Ø DATA -32768, 26Ø48,  16384,  5569,  13824
17Ø DATA   557Ø,    41,   5571,    32,   3Ø2Ø
18Ø DATA    772,-28143,-27184,   255,    257
19Ø DATA -27568, 32456,  26Ø48,    32,   9664
2ØØ DATA -32768,-32764,  17856,-32768,  26Ø48
21Ø DATA  16384, 324Ø4,   3Ø2Ø,   784,-3Ø692
22Ø DATA  1376Ø, 16384,    515,  5568,    154
23Ø DATA -3Ø7Ø6,-3Ø692,  1376Ø,    32,    536
24Ø DATA   5568,   156,-3Ø7Ø6,   276,    44Ø
25Ø DATA   55Ø5, 13761,     32,   515,   5568
26Ø DATA    156,-3Ø7Ø6,  13761, 16384,    515
27Ø DATA   5568,   154,-3Ø7Ø6.  55Ø6,   55Ø5
```

```
280 DATA -3Ø7ØØ,  5535,   176,    135, 26Ø52
29Ø DATA      2,  4869, -6716,      2,  5571
3ØØ DATA      1,  8396,   778,-23Ø83,   18Ø
31Ø DATA    765,-23Ø91,   184,    77Ø,  2691
32Ø DATA    5Ø2,  2764,   287,   5568,    32
33Ø DATA   557Ø,     9,  5569,     16,  5571
34Ø DATA     32,-3Ø7ØØ,-3Ø7Ø6,  3245Ø,  269Ø
35Ø DATA   9666,    13,   757,   557Ø,     9
36Ø DATA -3Ø7ØØ,-27328, 17856,   -256,-231Ø4
37Ø DATA    169.   517,-23Ø91,    18Ø,   772
38Ø DATA   269Ø.   5ØØ,-3Ø7Ø6,    499,-3Ø714
39Ø DATA   9664.     3.   514.   2572.   436
4ØØ DATA   9664.    27,   514.   27ØØ.   451
41Ø DATA   9664.    26,   754,   2764.  3Ø2Ø
42Ø DATA    7Ø1.  272Ø    493
43Ø FOR I%=Ø% TO &Ø6ØØ              ' Размещение текста HELP-драйвера
44Ø READ I1%                        ' в памяти, начиная с адреса
45Ø POKE &Ø32ØØØ+I%,I1%             '   &Ø32ØØØ
46Ø NEXT I%
47Ø DEF USRØ=&Ø32ØØØ
48Ø DATA "        Демонстрация работы♥         HELP-драйвера♥   Пос
ле установки экран♥  вызывается нажатием на кл. <Т♥♣"
49Ø DATA " Переход от одного HELP-экрана♥    к другому выполняет
ся с♥   помощью клавиш управления♥     курсором <вверх><вниз>♥♠"
5ØØ DATA "  Повторное нажатие на КТ♥   восстанавливает исходный
♥          экран♥♣"
51Ø DATA "    Для продолжения работы♥    нажмите сначала КТ, зат
ем♥     ВВОД, затем снова КТ♥♣♦"
52Ø DATA " HELP - драйвер позволяет выво-♥  дить в HELP-экраны р
азличные♥  сообщения в разных частях♥        Вашей программы♥♣"
53Ø DATA "  После установки HELP-драйвер♥    работает до его выг
рузки♥    как с активной программой,♥    так и при выходе в БЕЙС
ИК"
54Ø DATA "  Для правильного применения♥    HELP-драйвера исполь
зуйте♥ описание, а также текст данной♥          программы♥♣"
55Ø DATA "♥     Для завершения работы♥     нажмите сначала КТ, з
атем ВВОД♥♣♦"
56Ø RESTORE 48Ø
57Ø I1%=&Ø31ØØØ                     ' Размещение в памяти первого
58Ø GOSUB 2ØØØ                      ' HELP-текста с адреса &Ø31ØØØ
59Ø I1%=&Ø31ØØØ                     ' Установка
6ØØ I1%=USRØ(I1%)                   ' HELP-драйвера
61Ø I1%=174%                        ' Оформление
62Ø GOSUB 22ØØ                      ' экрана
63Ø B$=INKEY$                       '   Ожидание
64Ø IF B$="" THEN 63Ø               '   нажатия
65Ø IF ASC(B$)<>1Ø% THEN 63Ø        '   клавиши ВВОД
66Ø RESTORE 52Ø
67Ø I1%=&Ø3ØØØØ                     ' Размещение в памяти второго
68Ø GOSUB 2ØØØ                      ' HELP-текста с адреса &Ø3ØØØØ
69Ø I1%=&Ø3ØØØØ                     ' повторная установка
7ØØ I1%=USRØ(I1%)                   ' HELP-драйвера
71Ø I1%=178%                        ' Оформление
72Ø GOSUB 22ØØ                      ' экрана
73Ø B$=INKEY$                       '   Ожидание
74Ø IF B$="" THEN 73Ø               '   нажатия
75Ø IF ASC(B$)<>1Ø% THEN 73Ø        '   клавиши ВВОД
76Ø ? AT(63%,23%) CHR$(1Ø%)
77Ø ? AT(15%,23%) "ВЫГРУЖАТЬ HELP-ДРАЙВЕР (Y/N) ? ";
78Ø B$=INKEY$
79Ø IF (B$<>"Y")AND(B$<>"y")AND(B$<>"N")AND(B$<>"n") THEN 78Ø
8ØØ IF (B$="N")OR(B$="n") THEN END
81Ø I1%=Ø%                          ' Выгрузка
82Ø I1%=USRØ(I1%)                   ' HELP-драйвера
83Ø ?
84Ø ? AT(17%,23%) "HELP-ДРАЙВЕР ВЫГРУЖЕН"
85Ø END
2ØØØ READ A$
2Ø1Ø FOR I%=1% TO LEN(A$) STEP 2%
2Ø2Ø IF I%=LEN(A$) THEN J#=Ø ELSE J#=ASC(MID$(A$,I%+1%,1%))
2Ø3Ø J#=J#*256%+ASC(MID$(A$,I%,1%))
2Ø4Ø IF J#>=32767 THEN J#=J#-65536
2Ø5Ø I2%=I1%+I%-1%
2Ø6Ø POKE I2%,CINT(J#)
2Ø7Ø NEXT I%
2Ø8Ø I1%=I2%+2%
```

```
2090 IF MID$(A$,LEN(A$),1%)<>"♦" THEN 2000
2100 RETURN
2200 CLS
2210 FOR I%=1% TO 1472%
2220 ? CHR$(I1%);
2230 NEXT I%
2240 RETURN
```



НОВЫЙ СУПЕРЧИП ПОМОЖЕТ В СЛОЖНЫХ НАУЧНЫХ РАСЧЕТАХ

Американская фирма Intel, являющаяся крупнейшим производителем микросхем и снабжающая своей продукцией большинство персональных компьютеров, объявила о "суперчипе", который может превратить обычный персональный компьютер в мощную графическую станцию. ИС-860 — первая 64-бит микросхема, объединившая центральный процессор, графическое устройство и ЗУ на одной пластине кремния.

ИС-860 обладает в 30 раз большим быстродействием, чем нынешние ИС фирмы Intel и в 5 раз большим, чем ИС ее главного конкурента — фирмы Motorola.

Разработчики компьютеров планируют установку ИС в панель с задней стороны обычного персонального компьютера, и таким образом преобразовать его в научную рабочую станцию, способную выполнять сложные расчеты при моделировании динамических потоков или молекулярном моделировании.

В настоящее время выполнение сложных графических функций возможно лишь в режиме разделения времени на больших и очень дорогих суперкомпьютерах. ИС-860, стоящая 750 долл., может работать наравне со специальными графическими суперкомпьютерами, стоящими 100 000 долл.

Процессор-860 не предназначен для замены существующего набора ИС, микропроцессоров-286 и 386. Новая ИС будет играть роль ускорителя вычислений, работая вместе с процессором 386 или с ИС-486 в ПК.

ИС-860 превосходят все остальные благодаря использованию комбинации двух технологий. Первая известна под названием RISC - технологии (с ограниченным набором команд). Она позволяет преобразовывать сложные команды, требующие значительных затрат времени, в большее количество простых алгоритмов, которые могут быть быстро выполнены при определенной конфигурации компьютера. Эта специальная RISC-ИС может выполнять 80 млн. вычислений в секунду.

Вторая технология основана на физическом процессе, который позволяет Intel располагать компоненты на расстоянии 1 мкм друг от друга, используя технологию, известную как КМОП-технология.

860 использует ОС Unix для контроля функций микропроцессора. До сих пор никто не написал прикладных программ или программ, позволяющих пользователям разработать свои применения новых ИС.

Однако IBM сотрудничала с Intel в производстве дополнительной платы для компьютеров PS/2, стремясь получить преимущество в мощности от использования новой ИС. Microsoft компания, производящая большинство наиболее популярных программных средств для ПК, собирается разработать прикладные программы, которые смогут работать на ИС-860. Это даст фирме Intel значительное преимущество над всеми конкурентами, производящими ИС, основанные на RISC-технологии: над фирмой Motorola, производящей процессоры-8800, над Sun Microsystems, производящей Spare-ИС и над Mips Computers с ее RISC-ИС. Ни одна из этих конкурирующих фирм не получила столь больших выгод, какую дал союз IBM и Microsoft. Ян Уилсон, технический менеджер Intel по маркетингу, говорит, что его фирма работает также с группой компьютерных компаний, включающих Compag, Hewlett-Packard, Tandy и NEC, цель которых создать новую архитектуру для 32-бит ПК, названную EISA (архитектура расширенного промышленного стандарта). Она призвана создать конкуренцию "микроканальной" разработке фирмы IBM для шин, управляющих потоком данных внутри компьютера. Таким образом, новый процессор может быть использован в большей части следующего поколения компьютеров, построенных либо на микроканальной архитектуре, либо на архитектуре EISA. Итальянская группа Olivetti также планирует использовать в основе своей последней серии миникомпьютеров новые ИС.

До сих пор мощные процессоры окружались группой ИС "поддержки", каждая из которых выполняла свою, строго определенную роль, как, например, кристаллы памяти.

ИС-860, размер которой 10x15 см, содержит 1 млн. транзисторов или переключателей, что примерно в 4 раза больше, чем на существующих микропроцессорах. Эти дополнительные транзисторы означают, что 860 может иметь свою собственную кэш-память для работы с часто используемыми данными или программируемыми командами. Они позволяют также ИС-860 выполнять ряд других функций, которые ранее выполнялись ИС "поддержки". Например, эти транзисторы могут одновременно выполнять целочисленные вычисления над значащими цифрами числа и вычисления с плавающей запятой над незначащими цифрами числа.

ИС-860 может выполнять 150 млн. этих вычислений или "операций" в секунду с тактовой частотой 50 МГц. Это включает 100 операций с плавающей запятой и 50 целочисленных операций. Процессорам-386 для выполнения этих вычислений требовались отдельные модули. Кроме того, фирма Intel впервые создала ИС, которая может выполнять операцию менее чем за тактовый период, эквивалент пульсации в компьютере. ИС-860 может выполнить за это время три операции.

Том Мейер, менеджер по маркетингу 32-битных процессоров фирмы Motorola, главного конкурента Intel, заявил, что его фирма вряд ли выпустит новую ИС в следующем году.

New Scientist 1655 11.3.89. с.39

С.А.Утенков

МАЛОЕ ПРЕДПРИЯТИЕ "КОНУС"

предлагает русифицированные справочные руководства мгновенного доступа (формата Norton Guides), обучающие программы для IBM PC, а также методические разработки, содержащие подробные описания популярных программ.

Справочные руководства мгновенного доступа

Название	Цена (руб.)	Название	Цена (руб.)
CLIPPER	250	Norton Commander	50
Clipper tools one	120	Norton Guides	40
The Library for Clipper (Planet Software)	60	Norton Utility	40
		РЕБУС	130
SQLBASE for Clipper	60	PCTOOLS	90
Операционная система QNX	300	LEXICON v.6.57	40
RBASE-5000	75	BRIFF	40
EXEL for Windows:		Multiplan v.3.0	80
1. Getting Started		BTRIEVE	150
and Quick Reference	200	Super Calk v.5.0	150
2. Macro and Utilities	200	Xtalk	50
MS-KERMIT	200	Disk Manager	50
Novell SFT Advanced Netware		RS-232	30
286 v.2.15:		Dlink-IV	50
1. Users Reference Set	100	OS/2	120
2. Supervisor´s Guide	100	PKARC	50
3. Supervisor Reference	100	Fox Base	90
4. Console Reference	100	ASSEMBLER	120
5. Novell Installation Set	100	LOTUS 1-2-3	150
6. Novell Supplement´s	100	Turbo-Assembler	110
MS DOS для программистов	100	MS DOS v.4.1	100
Macro-Assembler	90	Vitamin-C	50
Turbo-Basic	90	MS C	60
Turbo-Pascal	100	RBASE SYSTEM V:	
FAST WIRE	40	1. Команды	70
LAPL-LINK	40	2. Ошибки	60
Procomm	40	PKARC	40
Справочник инженера-электроника		GW-BASIC	40
по эксплуатации персональных		QNX	120
компьютеров	120	REVELATION	90

Обучающие программы .

Название	Цена (руб.)	Название	Цена (руб.)
DOS Help v.3.20	120	RBASE	210
Norton Integrator	110	Dbase-IV	120
Super Calk v.5.0	110	Frame-Work-III	120
LOTUS 1-2-3	110	Btrieve	120
GW-MOUSE	100	MS C	100
Операционная система реального времени QNX	300	DOS Help v.3.30	120

Условия поставки:

1. Предоплата на р/с 240905 в Ленинградском филиале МИБ г.Москвы МФО 201069.
2. В наш адрес выслать письмо с вашим почтовым адресом, перечнем программ и пособий и копию платежного поручения.

Наш адрес: 125171, Москва, Ленинградское шоссе, д.18.
Телефон для справок: 150-85-07

Ф 38 Файл заражен! — М.: Знание, 1991. — 48 с. — (Новое в жизни, науке, технике. Сер. "Вычислительная техника и ее применение"; № 8).
ISBN 5-07-001720-9
35 к.

Проблема защиты информации от вирусов, защиты от неквалифицированных действий, от случайной порчи и стирания — главная тема этого выпуска. Много внимания уделено восстановлению утраченной информации.

Материал рассчитан на широкий круг читателей.

2302030000 ББК 32.85



Научно-популярное издание

ФАЙЛ ЗАРАЖЕН!

Зам. главного редактора *Г. Г. Карвовский*
Редактор *Б. М. Васильев*
Мл.редактор *Н. А. Васильева*
Художник *В. Н. Конюхов*
Худож.редактор *И. А. Емельянова*
Техн.редактор *Т. В. Луговская*
Корректор *В. И. Гуляева*

ИБ № 11727

Подписано к печати 21.06.91. Формат бумаги 70x100 1/16. Бумага офсетная. Печать офсетная. Усл.печ.л.3,90. Усл.кр.-отт.8,45. Уч.-изд.л.4,67. Тираж 49635 экз. Заказ 2260. Цена 35 коп. Издательство "Знание". 101835, ГСП, Москва, Центр, проезд Серова,д.4. Индекс заказа 914708. Отпечатано с оригинал-макета, подготовленного издательством "Знание" в издательской системе Xerox Ventura Publisher (ОС MS DOS), на ордена Трудового Красного Знамени Тверском полиграфическом комбинате Государственного комитета СССР по печати. 170024, г.Тверь, пр.Ленина,5.

Цена 35 коп. Индекс 70195

Адрес подписчика:
сол. 5-27



Подписная
научно-
популярная
серия

ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
И ЕЕ ПРИМЕНЕНИЕ

Машина пятого поколения должна работать так, чтобы во всем соответствовать человеку, в противоположность сложившейся ситуации, когда человек должен осваивать машину, подлаживаться под нее и следовать ее правилам.

Хадзамо Корацу

Все знают, что компьютер ошибиться не может. Но не все знают, что он может быть сознательно запрограммирован на ошибку.

А.Хейли

*Наш адрес:
101835,
Москва,
Центр,
проезд
Серова, 4*